Journal of Algebra **247,** 370–434 (2002)
doi:10.1006/jabr.2001.9016, available online at http://www.idealibrary.com on IDEAL®

Prime Power Graphs for Groups of Lie Type[1]

William M. Kantor

University of Oregon, Eugene, Oregon 97403

Ákos Seress

The Ohio State University, Columbus, Ohio 43210

Communicated by Gernot Stroth

Received September 28, 2000

We associate a weighted graph $\Delta(G)$ to each finite simple group G of Lie type. We show that, with an explicit list of exceptions, $\Delta(G)$ determines G up to isomorphism, and for these exceptions, $\Delta(G)$ nevertheless determines the characteristic of G.

This result was motivated by algorithmic considerations. We prove that for any finite simple group G of Lie type, input as a black-box group with an oracle to compute the orders of group elements, $\Delta(G)$ and the characteristic of G can be computed by a Monte Carlo algorithm in time polynomial in the input length. The characteristic is needed as part of the input in a previous constructive recognition algorithm for G. © 2002 Elsevier Science

1. INTRODUCTION

For each finite simple group G of Lie type of characteristic p, define a graph $\Gamma(G)$ as follows. The vertices of $\Gamma(G)$ are the prime powers r^a that occur as orders of some elements of G, for all primes $r \neq p$ and integers $a > 0$. Prime powers r^a, s^b are connected if and only if G has an element of order $\mathrm{lcm}(r^a, s^b)$ (thus, every vertex of $\Gamma(G)$ has a loop). We say that two vertices of $\Gamma(G)$ are *equivalent* if they have the same neighbors, and we denote the quotient graph with respect to this equivalence relation by $\Delta(G)$; the vertex set of $\Delta(G)$ is denoted $V(\Delta(G))$. We consider $\Delta(G)$ as a

[1] This research was supported in part by the National Science Foundation.

0021-8693/02 $35.00

simple graph (i.e., without loops and multiple edges) and as a *weighted graph*: the *weight* of $v \in V(\Delta(G))$ is the least common multiple of the prime powers in the equivalence class v.

Since $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$, $\mathrm{PSL}(3,2) \cong \mathrm{PSL}(2,7)$, $\mathrm{PSU}(4,2) \cong \Omega(5,3)$, $\mathrm{PSL}(2,9) \cong \mathrm{Sp}(4,2)'$, $G_2(2)' \cong \mathrm{PSU}(3,3)$, and ${}^2G_2(3)' \cong \mathrm{PSL}(2,8)$, the group does not necessarily determine the characteristic uniquely. Thus, in these cases, the above description provides us with two different graphs $\Gamma(G)$.

The main purpose of this paper is to investigate whether the weighted graph $\Delta(G)$ determines G. We shall prove the following theorem.

THEOREM 1.1. *Let G and G^* be finite simple groups of Lie type such that $\Delta(G) \cong \Delta(G^*)$. Then $G \cong G^*$ unless the pair $\{G, G^*\}$ is one of the following*:

(i) $\{G, G^*\} = \{\mathrm{PSp}(2m, q), \Omega(2m+1, q)\}$ *for $m \geq 5$ and q odd*,

(ii) $\{G, G^*\} = \{\mathrm{PSp}(4, q), \mathrm{PSL}(2, q^2)\}$,

(iii) $\{G, G^*\} \subseteq \{\mathrm{PSp}(6, q), \mathrm{P}\Omega^+(8, q), \Omega(7, q)\}$,

(iv) $\{G, G^*\} \subseteq \{\mathrm{PSp}(8, q), \mathrm{P}\Omega^-(8, q), \Omega(9, q)\}$, *or*

(v) $\{G, G^*\} = \{\mathrm{PSL}(3, 2), G_2(2)'\}$,

in which case G and G^* have the same characteristic.

Of course, in (iii) and (iv) the first and last groups are isomorphic when q is even. The proof is based on information concerning maximal tori of G as well as a very careful examination of orders of elements. In Section 2, we describe the graphs $\Delta(G)$ for the exceptional groups. In Section 3, we collect information about $\Delta(G)$ for classical groups. The proof of Theorem 1.1 is in Section 4.

Theorem 1.1 was motivated by algorithmic considerations. In [KS1] we gave a constructive black-box recognition algorithm for the classical simple groups; [KM] does this for the exceptional groups of Lie type. However, in both papers the characteristic of the group was part of the input. Now Theorem 1.1 allows us to compute the characteristic. In Section 5, we give the necessary algorithmic background and prove the following theorem.

THEOREM 1.2. *For any finite simple group G of Lie type, given as a black-box group with an oracle for the computation of the orders of group elements, $\Delta(G)$ and the characteristic can be found by a Monte Carlo algorithm in time polynomial in the input length*.

The proof of Theorem 1.2, which we shall describe in Section 5.3, does not provide a practical algorithm. Therefore, in Section 5.4, we shall indicate a heuristic shortcut and a conjecture which would make this shortcut a precise argument.

The graph $\Gamma(G)$ is related to the somewhat more familiar *prime graph* of G, whose vertices are all of the prime divisors of $|G|$, with different

vertices joined if and only if there is an element whose order is the product of the primes. The literature concerning prime graphs mostly deals with their number of components [Wi, Ko, IY, Lu]. We are interested in $\Delta(G)$ instead of the prime graph because of the algorithmic applications: we can construct $\Delta(G)$ in polynomial time, by a Monte Carlo algorithm, but we cannot construct the prime graph (since that would require the ability to factor integers, which we do not presuppose). The number of connected components is the same in $\Gamma(G)$ and $\Delta(G)$, and in most cases this is the same as in the prime graph of G.

2. THE GRAPHS OF EXCEPTIONAL GROUPS

Lists of maximal tori are in print for all exceptional groups. Since each semisimple element of G occurs as an element of some maximal torus of G, it is straightforward to determine $\Delta(G)$ from these lists.

For each exceptional group, we list the maximal tori and the *adjacency matrix* of $\Delta(G)$. The rows and columns of the adjacency matrix correspond to the vertices of $\Delta(G)$. The entry (i, j) of the matrix is 1 if there is an edge between the ith and jth vertex, and it is 0 otherwise. We labeled the rows of the adjacency matrix by the weights of the corresponding vertices. For small values of the size of the underlying field, or if the field size satisfies certain divisibility conditions, some listed weights may be equal to 1. This means that these vertices do not exist. We denote such weights by an asterisk $(*)$.

For a prime p, as usual a_p denotes the largest power of p dividing a. In the following lists, the notation a means a cyclic group of order a and $a \times b$ denotes the direct product of cyclic groups of order a and b. In the computation of vertex weights we use the following elementary facts:

$$(q^i - 1, q^j - 1) = q^{(i,j)} - 1 \qquad \text{and} \qquad \left(\frac{q^d - 1}{q - 1}, q - 1\right) = (d, q - 1). \tag{2.1}$$

We will need integers associated with $\Delta(G)$ for all groups of Lie type:

DEFINITION 2.2.

$L_2(G)$ = lcm of the weights of vertices of valency $|V(\Delta(G))| - 2$;

$L_3(G)$ = lcm of the weights of vertices of valency *at least* $|V(\Delta(G))| - 3$;

$L(G)$ = lcm of the weights of vertices of valency *at least* $|V(\Delta(G))| - 3$ as well as the powers of 3 occurring in the weights of vertices of valency $|V(\Delta(G))| - 4$.

2.1. ${}^2B_2(q)$

Maximal tori in ${}^2B_2(q)$, $q = 2^{2m+1}$ for some $m \geq 1$ [Suz].

$$q - 1,$$
$$q + \sqrt{2q} + 1$$
$$q - \sqrt{2q} + 1$$

The graph $\Delta({}^2B_2(q))$:

$$\begin{matrix} q - 1 \\ q + \sqrt{2q} + 1 \\ q - \sqrt{2q} + 1 \end{matrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

2.2. ${}^2G_2(q)$

The graph $\Delta({}^2G_2(3)')$ [CCNPW]:

$$\begin{matrix} 2 \\ 7 \end{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Maximal tori in ${}^2G_2(q)$, $q = 3^{2m+1}$ for some $m \geq 1$ [Wa].

$$q - 1$$
$$(q + 1)/2 \times 2$$
$$q + \sqrt{3q} + 1$$
$$q - \sqrt{3q} + 1$$

The graph $\Delta({}^2G_2(q))$:

$$\begin{matrix} (q - 1)/2 \\ 2 \\ (q + 1)/2 \\ q + \sqrt{3q} + 1 \\ q - \sqrt{3q} + 1 \end{matrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2.3. $G_2(q)$

The graph $\Delta(G_2(2)')$ [CCNPW]:

$$\begin{matrix} 3 \\ 7 \end{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Maximal tori in $G_2(q)$, $q \geq 3$ [Asch2].

$$
\begin{array}{l}
(q-1) \times (q-1) \\
q^2 - 1 \\
(q+1) \times (q+1) \\
q^2 - q + 1 \\
q^2 + q + 1
\end{array}
$$

The graph $\Delta(G_2(q))$:

$$
\begin{array}{r}
(q^2-1) \cdot (9, q^2-1)/(3, q^2-1)^2 \\
(q^2 - q + 1)/(3, q+1) \\
(q^2 + q + 1)/(3, q-1) \\
(3, q-1)* \\
(3, q+1)*
\end{array}
\begin{pmatrix}
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0
\end{pmatrix}
$$

2.4. ${}^3D_4(q)$

Maximal tori in ${}^3D_4(q)$ [DM].

$$
\begin{array}{l}
(q-1) \times (q^3-1) \\
(q+1) \times (q^3+1) \\
(q^3-1)(q+1) \\
(q^3+1)(q-1) \\
(q^2+q+1) \times (q^2+q+1) \\
(q^2-q+1) \times (q^2-q+1) \\
q^4 - q^2 + 1
\end{array}
$$

The graph $\Delta({}^3D_4(q))$:

$$
\begin{array}{r}
(q^2 - q + 1) \cdot (q+1)_3 \\
q^2 - 1 \\
(q^2 + q + 1) \cdot (q-1)_3 \\
q^4 - q^2 + 1
\end{array}
\begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
$$

2.5. ${}^2F_4(q)$

The graph $\Delta({}^2F_4(2)')$ [CCNPW]:

$$\begin{array}{r} 3 \\ 5 \\ 13 \end{array}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Maximal tori in ${}^2F_4(q)$, $q = 2^{2m+1}$ for some $m \geq 1$ [Shi2].

$$\begin{array}{l} (q-1) \times (q-1) \\ q^2 - 1 \\ (q-1) \times \left(q - \sqrt{2q} + 1\right) \\ (q-1) \times \left(q + \sqrt{2q} + 1\right) \\ q^2 + 1 \\ \left(q - \sqrt{2q} + 1\right) \times \left(q - \sqrt{2q} + 1\right) \\ \left(q + \sqrt{2q} + 1\right) \times \left(q + \sqrt{2q} + 1\right) \\ (q+1) \times (q+1) \\ q^2 - q + 1 \\ q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1 \\ q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1 \end{array}$$

The graph $\Delta({}^2F_4(q))$:

$$\begin{array}{r} q-1 \\ q+1 \\ q^2+1 \\ q^2-q+1 \\ q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1 \\ q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1 \end{array}\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2.6. $F_4(q)$

Maximal tori in $F_4(q)$ [Shi1, Sho]; see [La, pp. 94–96, 99] for the precise structure of the tori when q is odd.

$(q-1) \times (q-1) \times (q-1) \times (q-1)$

$(q-1) \times (q-1) \times (q^2-1)$ (two conjugacy classes)

$(q-1)\times(q+1)\times(q^2-1)$
$(q^2-1)\times(q^2-1)$
$(q-1)\times(q^3-1)$ (two conjugacy classes)
$(q-1)\times(q-1)(q^2+1)$
$(q+1)\times(q+1)\times(q^2-1)$ (two conjugacy classes)
$(q-1)\times(q^2+1)(q+1)$
$(q^4-1)/(2,q-1)\times(2,q-1)$
$(q^3+1)(q-1)$ (two conjugacy classes)
$(q^3-1)(q+1)$ (two conjugacy classes)
$(q+1)\times(q+1)\times(q+1)\times(q+1)$
$(q^2+q+1)\times(q^2+q+1)$
$(q+1)\times(q^2+1)(q+1)$
$(q+1)\times(q^3+1)$ (two conjugacy classes)
$(q^2+1)\times(q^2+1)$
q^4+1
q^4-q^2+1
$(q^2-q+1)\times(q^2-q+1)$

The graph $\Delta(F_4(q))$:

$$\begin{array}{r|ccccccc}
(2,q-1)* & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
q^2-1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
(q^2+1)/(2,q-1) & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
(q^2+q+1)\cdot(q-1)_3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
(q^2-q+1)\cdot(q+1)_3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
(q^4+1)/(2,q-1) & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
q^4-q^2+1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

2.7. $E_6(q)$

Maximal tori in $(3,q-1).E_6(q)$ [DF].

$(q-1)\times(q-1)\times(q-1)\times(q-1)\times(q-1)\times(q-1)$
$(q-1)\times(q-1)\times(q-1)\times(q-1)\times(q^2-1)$
$(q-1)\times(q-1)\times(q^2-1)\times(q^2-1)$
$(q-1)\times(q-1)\times(q-1)\times(q^3-1)$
$(q^2-1)\times(q^2-1)\times(q^2-1)$

$(q-1)\times(q^2-1)\times(q^3-1)$
$(q-1)\times(q-1)\times(q^4-1)$
$(q+1)\times(q+1)\times(q^2-1)\times(q^2-1)$
$(q^2-1)\times(q+1)(q^3-1)$
$(q-1)\times(q^2+q+1)\times(q^3-1)$
$(q^2-1)\times(q^4-1)$
$(q-1)\times(q^5-1)$
$(q^2-1)\times(q-1)(q^3+1)$
$(q-1)(q^2+1)\times(q-1)(q^2+1)$
$(q^2+q+1)\times(q+1)(q^3-1)$
$(q+1)\times(q+1)\times(q^4-1)$
$(q+1)(q^5-1)$
$(q^2+q+1)\times(q-1)(q^3+1)$
$(q^2-1)(q^4+1)$
$(q-1)(q^2+1)(q^3+1)$
$(q^2+q+1)\times(q^2+q+1)\times(q^2+q+1)$
$(q+1)\times(q^5+q^4+q^3+q^2+q+1)$
$(q^2+q+1)(q^4-q^2+1)$
q^6+q^3+1
$(q^2-q+1)\times(q^4+q^2+1)$

The graph $\Delta(E_6(q))$:

$$\begin{array}{r|cccccccccccc}
(q^2-1)/(3,q-1) & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
(q^2+1)/(2,q-1) & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
(q^2-q+1)\cdot(q+1)_3 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
(q^2+q+1)/(3,q-1) & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
(q^4+1)/(2,q-1) & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
(q^4+q^3+q^2+q+1)\cdot(q-1)_5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
q^4-q^2+1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(q^6+q^3+1)/(3,q-1) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(q-1)_3* & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
(3,q-1)\cdot(q-1)_3* & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
(2,q-1)\cdot(q^2-1)_2* & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

2.8. ${}^2E_6(q)$

The list of maximal tori of $(3, q+1)\cdot {}^2E_6(q)$ can be obtained from the list in Section 2.7 by replacing q by $-q$ [DF]. Consequently, the graph $\Delta({}^2E_6(q))$ is isomorphic to $\Delta(E_6(q))$, and the weights are obtained by replacing q by $-q$ in the weights of $\Delta(E_6(q))$.

The graph $\Delta({}^2E_6(q))$ (if $q = 2$ then vertex 4 does not exist, and so vertices 2, 3 become equivalent):

$$\begin{array}{rc}
(q^2-1)/(3,q+1)* & \begin{pmatrix}0&1&1&1&1&1&0&0&1&1&1\end{pmatrix}\\
(q^2+1)/(2,q-1) & \begin{pmatrix}1&0&1&0&0&0&0&0&1&0&1\end{pmatrix}\\
(q^2+q+1)\cdot(q-1)_3 & \begin{pmatrix}1&1&0&1&0&0&0&0&1&0&1\end{pmatrix}\\
(q^2-q+1)/(3,q+1)* & \begin{pmatrix}1&0&1&0&0&0&1&0&1&1&0\end{pmatrix}\\
(q^4+1)/(2,q-1) & \begin{pmatrix}1&0&0&0&0&0&0&0&0&0&1\end{pmatrix}\\
(q^4-q^3+q^2-q+1)\cdot(q+1)_5 & \begin{pmatrix}1&0&0&0&0&0&0&0&1&0&0\end{pmatrix}\\
q^4-q^2+1 & \begin{pmatrix}0&0&0&1&0&0&0&0&0&0&0\end{pmatrix}\\
(q^6-q^3+1)/(3,q+1) & \begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0\end{pmatrix}\\
(q+1)_3* & \begin{pmatrix}1&1&1&1&0&1&0&0&0&1&0\end{pmatrix}\\
(3,q+1)\cdot(q+1)_3* & \begin{pmatrix}1&0&0&1&0&0&0&0&1&0&0\end{pmatrix}\\
(2,q-1)\cdot(q^2-1)_2* & \begin{pmatrix}1&1&1&0&1&0&0&0&0&0&0\end{pmatrix}
\end{array}$$

2.9. $E_7(q)$

Maximal tori in $(2, q-1)\cdot E_7(q)$ [DF].

$(q-1)\times$ items from the list in Section 2.7
$(q-1)\times(q+1)\times(q+1)\times(q^2-1)\times(q^2-1)$
$(q-1)\times(q^3-1)\times(q^3-1)$
$(q-1)\times(q^2-1)\times(q^4-1)$
$(q^3-1)\times(q+1)(q^3-1)$
$(q-1)\times(q+1)\times(q+1)\times(q^4-1)$
$(q-1)\times(q+1)(q^5-1)$
$(\mathrm{q}-1)\times(q^6-1)$
$(q-1)\times(q^2-1)(q^4+1)$
$(q^2+q+1)\times(q^2+q+1)\times(q^3-1)$
$(q^3+1)\times(q^3-1)\times(q+1)$
$(q^3-1)(q^4-q^2+1)$
$(q-1)(q^6+q^3+1)$

$(q^2 - q + 1) \times (q - 1)(q^4 + q^2 + 1)$
$(q^3 - 1) \times (q^4 - 1)$
$(q^5 - 1)(q^2 + q + 1)$
$(q - 1)(q^2 + 1) \times (q^2 - 1) \times (q^2 + 1)$
$q^7 - 1$
$(q^4 + 1) \times (q - 1)(q^2 + 1)$

Also orders obtained by replacing q by $-q$ in the above lists.

The graph $\Delta(E_7(q))$:

$(q-1)/(2,q-1)*$	0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1
$(q+1)/(2,q-1)$	1 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1
$(q^2+1)/(2,q-1)$	1 1 0 1 1 1 0 0 0 0 0 0 0 1 1 1 1
$(q^2+q+1)/(3,q-1)$	1 1 1 0 1 0 1 0 1 0 0 0 0 1 1 1 1
$(q^2-q+1)/(3,q+1)*$	1 1 1 1 0 0 1 1 0 0 0 0 0 1 1 1 1
$(q^4+1)/(2,q-1)$	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1
q^4-q^2+1	1 1 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0
$(q+1)_5 \cdot (q^5+1)/(q+1)$	1 1 0 0 1 0 0 0 0 0 0 0 0 0 1 1 0
$(q-1)_5 \cdot (q^5-1)/(q-1)$	1 1 0 1 0 0 0 0 0 0 0 0 0 1 0 1 0
$(q^6-q^3+1)/(3,q+1)$	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0
$(q^6+q^3+1)/(3,q-1)$	1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
$(q+1)_7 \cdot (q^7+1)/(q+1)$	0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$(q-1)_7 \cdot (q^7-1)/(q-1)$	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$(3,q-1) \cdot (q-1)_3*$	1 1 1 1 1 0 1 0 1 0 1 0 0 0 0 1 1
$(3,q+1) \cdot (q+1)_3*$	1 1 1 1 1 0 1 1 0 1 0 0 0 0 0 1 1
$(q^2-1)_2*$	1 1 1 1 1 1 0 1 1 0 0 0 0 1 1 0 1
$(2,q-1) \cdot (q^2-1)_2*$	1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 0

2.10. $E_8(q)$

Maximal tori in $E_8(q)$ [DF].

$(q - 1) \times$ items from the list in Section 2.9
$(q - 1) \times (q^3 - 1) \times (q^4 - 1)$
$(q - 1) \times (q^5 - 1)(q^2 + q + 1)$
$(q^2 - 1) \times (q^2 + 1)(q - 1) \times (q^2 + 1)(q - 1)$
$(q - 1) \times (q^7 - 1)$

$(q-1)(q^4+1) \times (q-1)(q^2+1)$
$(q^2-1) \times (q^2-1) \times (q^2-1) \times (q^2-1)$
$(q^2-1) \times (q^2-1) \times (q+1)(q^3-1)$
$(q^2-1) \times (q^2-1) \times (q^4-1)$
$(q+1)(q^3-1) \times (q+1)(q^3-1)$
$(q+1)(q^3-1) \times (q^4-1)$
$(q^4-1) \times (q^4-1)$
$(q^2-1) \times (q^2-1) \times (q^2+1) \times (q^2+1)$
$(q^2-1) \times (q+1)(q^5-1)$
$(q^2-1) \times (q^6-1)$ (two conjugacy classes)
$(q-1)(q^2+1) \times (q^2+1)(q^3-1)$
$(q^2-1) \times (q^2-1)(q^4+1)$
$(q^2+q+1) \times (q^2+q+1) \times (q+1)(q^3-1)$
$(q+1)(q^2+q+1)(q^5-1)$
$(q+1)(q^2+1)(q^5-1)$
$(q+1)(q^7-1)$
q^8-1
$(q^2-1) \times (q^2+1) \times (q^4+1)$
$(q^2+1) \times (q^2+1) \times (q^4-1)$
$(q+1)(q^3-1)(q^4+1)$
$(q^2+1)(q^6-1)$
$(q^2-1)(q^2+q+1)(q^4-q^2+1)$
$(q^2-1)(q^6+q^3+1)$
$(q^2-q+1) \times (q^2-q+1) \times (q+1)(q^3-1)$
$(q^2-1)(q^6+1)$
$(q^2+q+1) \times (q^2+q+1) \times (q^2+q+1) \times (q^2+q+1)$
$(q^4+q^3+q^2+q+1) \times (q^4+q^3+q^2+q+1)$
$(q^2+q+1) \times (q^6+q^3+1)$
$(q^2+1) \times (q^2+1) \times (q^2+1) \times (q^2+1)$
$(q^2+1) \times (q^6+1)$
$(q^4+1) \times (q^4+1)$
$(q^4-q^2+1)(q^2+q+1) \times (q^2+q+1)$
$(q^4+q^2+1) \times (q^2+q+1) \times (q^2-q+1)$
$q^8+q^7-q^5-q^4-q^3+q+1$

$q^8 - q^4 + 1$
$q^8 - q^6 + q^4 - q^2 + 1$
$(q^4 - q^2 + 1) \times (q^4 - q^2 + 1)$

Also orders obtained by replacing q by $-q$ in the above lists.

The graph $\Delta(E_8(q))$:

$q^2 - 1$	0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1
$(q^2 + 1)/(2, q - 1)$	1 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1
$(q^2 + q + 1)/(3, q - 1)$	1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 1 1 1 0
$(q^2 - q + 1)/(3, q + 1)*$	1 1 1 0 1 1 1 0 1 0 0 0 0 0 0 0 1 1 1 0
$(q^4 + 1)/(2, q - 1)$	1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1
$q^4 - q^2 + 1$	1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0
$(q + 1)_5 \cdot (q^5 + 1)/(q + 1)$	1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0
$(q - 1)_5 \cdot (q^5 - 1)/(q - 1)$	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0
$(q^6 - q^3 + 1)/(3, q + 1)$	1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0
$(q^6 + q^3 + 1)/(3, q - 1)$	1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
$(q + 1)_7 \cdot (q^7 + 1)/(q + 1)$	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$(q - 1)_7 \cdot (q^7 - 1)/(q - 1)$	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$q^8 - q^4 + 1$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$q^8 - q^6 + q^4 - q^2 + 1$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$(3, q - 1) \cdot (q - 1)_3*$	1 1 1 1 1 1 0 1 0 1 0 0 0 0 0 0 0 1 0
$(3, q + 1) \cdot (q + 1)_3*$	1 1 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 1 0
$(2, q - 1) \cdot (q^2 - 1)_2*$	1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 1
$(2, q - 1)^2 \cdot (q^2 - 1)_2*$	1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0

In view of the above graphs, we note the following properties:

PROPOSITION 2.3. (i) *The exceptional groups with* $|V(\Delta(G))| \geq 7$ *are* $F_4(q)$ *with* q *odd*, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, *and* $E_8(q)$.

(ii) *If* $|V(\Delta(G))| \geq 7$ *then* $L_2(G) = 1$ *except when* G *is* $F_4(q)$ *with* q *odd*.

3. THE GRAPHS OF THE CLASSICAL GROUPS

In this section we collect the properties of the graphs of the classical groups needed in the proof of Theorem 1.1 given in Section 4. Although the structure of maximal tori is well-known in these groups, we mostly use a different methodology: for each pair $\{r^a, s^b\}$ of prime powers adjacent in $\Gamma(G)$, an element of order $\mathrm{lcm}(r^a, s^b)$ occurs already in a torus that is a product of at most two cyclic groups, so considering all tori is not necessary. Instead, we work with a slight generalization of the notion of primitive prime divisors [Zs]. The major difficulty is to handle the powers of those primes that are factored out when passing from a linear group to the corresponding projective group.

Let G and $\hat{G}$ denote the following groups, where $q = p^e$:

G	$\mathrm{PSL}(d,q)$	$\mathrm{PSp}(2m,q)$, $m \geq 2$	$\mathrm{P}\Omega^\varepsilon(d,q)$, $d \geq 7$	$\mathrm{PSU}(d,q)$, $d \geq 3$
$\hat{G}$	$\mathrm{SL}(d,q))$	$\mathrm{Sp}(2m,q)$	$\Omega^\varepsilon(d,q)$	$\mathrm{SU}(d,q)$.

Here ε is deleted if d is odd, in which case we may also assume that q is odd; if d is even then $\varepsilon \in \{+,-\}$.

Write $Z = Z(\hat{G})$.

Let V denote the vector space underlying $\hat{G}$. The symbols V_i and W_i always denote subspaces of V of dimension i.

Let $\mathbf{C}(r^a)$ denote the vertex of $\Delta(G)$ (i.e., equivalence class) determined by the prime power r^a; its valency is denoted $v(\mathbf{C}(r^a))$.

3.1. $\mathrm{PSL}(d,q)$

For each classical group we will have to determine the vertices of $\Gamma(G)$ and a parametrization of them. For this purpose we use the following definition in the $\mathrm{PSL}(d,q)$ case as well as analogous ones for the other classical groups:

DEFINITION 3.1. If $1 \leq i \leq d$ we say that a prime power $r^a > 1$ is an $\mathrm{lpppd}^{\#}(q;i,d)$-*number* (a *linear primitive prime power divisor*) if one of the following holds:

- for $i < d-1$, r^a is $\mathrm{lpppd}^{\#}(q;i,d)$ if $r^a \mid q^i - 1$ but $r^a \nmid q^j - 1$ for any $1 \leq j < i$;
- for $i = d-1$, r^a is $\mathrm{lpppd}^{\#}(q;d-1,d)$ if $r^a \mid (q^{d-1}-1)/(q-1,d)$ but $r^a \nmid q^j - 1$ for any $1 \leq j < d-1$;
- for $i = d$, r^a is $\mathrm{lpppd}^{\#}(q;d,d)$ if $r^a \mid (q^d-1)/((q-1)(q-1,d))$ but $r^a \nmid q^j - 1$ for $1 \leq j < d$.

Note that the above cases are mutually exclusive, since $(q^{d-1}-1)/(q-1,d)$ and $(q^d-1)/(q-1)(q-1,d)$ are relatively prime. This already

suggests that difficulties may arise in using this definition (and similar ones later on) when $r \mid (q-1, d)$; these lead us to careful examinations of some abelian subgroups of the projective group G.

The above definition is a variation of the notion of a *primitive prime divisor*: for primes p and r and an integer $k \geq 1$, we say that r is a ppd$(p; k)$-*prime* if $r \mid p^k - 1$ but $r \nmid p^j - 1$ for all $1 \leq j < k$. By a theorem of Zsigmondy [Zs], for all p, k there are ppd$(p; k)$-primes with two exceptions: (i) $p = 2$, $k = 6$; and (ii) p is a Mersenne prime and $k = 2$. In particular, Zsigmondy's Theorem implies that lpppd$^{\#}(q; i, d)$-numbers exist for any q, i, d as in the above definition, except when $q = 2$ and $i = 1$, or $q = 3$, $d = 2$ and $i \in \{1, 2\}$.

If GL(k, q) has an irreducible element of order r^a a power of a prime $r \neq p$, then (by Schur's Lemma) $r^a \mid q^k - 1$ but $r^a \nmid q^j - 1$ for $1 \leq j < k$. Thus, r^a uniquely determines k as the order of $q \pmod{r^a}$.

PROPOSITION 3.2. *The vertices of* $\Gamma(\mathrm{PSL}(d, q))$ *are the* lpppd$^{\#}(q; i, d)$-*numbers*.

Proof. For $i \leq d-1$, write $V = V_i \oplus V_1 \oplus W_{d-i-1}$ and let $\langle x \rangle \times \langle y \rangle < \mathrm{GL}(d, q)$, where x and y act as Singer cycles (of order $q^i - 1$ and $q - 1$) on V_i and V_1 while inducing 1 on $V_1 \oplus W_{d-i-1}$ and $V_i \oplus W_{d-i-1}$, respectively. For each $x' \in \langle x \rangle$ there is a unique $y_{x'} \in \langle y \rangle$ with $\det(x' y_{x'}) = 1$, so that $x' y_{x'} \in \hat{G}$.

First suppose that r^a is an lpppd$^{\#}(q; i, d)$-number with $1 \leq i \leq d-2$. Then xy_x has order $q^i - 1$ and fixes a nonzero vector in W_{d-i-1}, so the element of $\langle xy_x \rangle$ of order r^a projects onto an element of G of the same order.

Next consider an lpppd$^{\#}(q; d-1, d)$-number r^a. This time $xy_x \in \hat{G}$ has order $q^{d-1} - 1$. Since $|Z| = (d, q-1)$, we see that $xy_x Z \in G$ has order $(q^{d-1} - 1)/(d, q-1)$ and hence has a power of order r^a.

Finally, if r^a is an lpppd$^{\#}(q; d, d)$-number, let $x \in \mathrm{GL}(d, q)$ have order $q^d - 1$. Then $x^{q-1} \in \hat{G}$ has order $(q^d - 1)/(q-1)$, so $x^{q-1} Z \in G$ has order $(q^d - 1)/(q-1)(q-1, d)$ and one of its powers has order r^a.

Conversely, suppose that $g \in G$ has order r^a for a prime $r \neq p$. If $g = hZ$ with $h \in \hat{G}$ an r-element, then V is the direct sum of subspaces on each of which h acts irreducibly; moreover, h is faithful on at least one of these subspaces W. Let $i = \dim W$. By Schur's Lemma, $|h| \mid q^i - 1$, but $|h| \nmid q^j - 1$ for $j < i$, so $|h|$ is lpppd$^{\#}(q; i, d)$ if $i \leq d-2$. Since $r^a \mid |h|$, r^a is also an lpppd$^{\#}(q; i', d)$ for some $i' \mid i$. If $i = d - 1 > 1$ then $r \nmid (d, q-1)$ and hence $|h| = r^a$ and $r^a \mid (q^{d-1} - 1)/(d, q-1)$ (for, if $r \mid (d, q-1)$ then $(q-1)_r = (q^{d-1} - 1)_r$ by (2.1), and hence W has a 1-dimensional h-invariant subspace). If $i = d - 1 = 1$ then the order of any semisimple element divides $(q \pm 1)/(2, q-1)$. Finally, if $i = d$ then $C_{\mathrm{PSL}(d,q)}(g)$ is

part of a Singer cycle of $\mathrm{PGL}(d,q)$ and hence has order $(q^d-1)/(q-1)(d,q-1)$, which must therefore be divisible by r^a. ∎

We now turn to edges. Here and in later sections r and s will denote primes that are not assumed to be distinct.

PROPOSITION 3.3. *Let r^a be $\mathrm{lpppd}^{\#}(q;i,d)$ and let s^b be $\mathrm{lpppd}^{\#}(q;j,d)$ for some i,j with $1 \le i \le j \le d$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{PSL}(d,q))$ if and only if one of the following holds*:

(i) $i+j<d$,

(ii) $i+j=d$ *and* $2 \le i \le j \le d-2$,

(iii) $i \mid j$ *and* $j \le d-2$,

(iv) $j=d-1$, $i \mid d-1$, *and* $r^a \mid (q^{d-1}-1)/(q-1,d)$, *or*

(v) $j=d$, $i \mid d$, *and* $r^a \mid (q^d-1)/((q-1)(q-1,d))$.

Proof. First we show that if r^a and s^b satisfy at least one of the conditions (i)–(v), then they are adjacent in $\Gamma(\mathrm{PSL}(d,q))$.

If $i \mid j$ then $r^a \mid q^j-1$. As we saw in the proof of Proposition 3.2, G has an element w of order q^j-1, $(q^{d-1}-1)/(d,q-1)$, or $(q^d-1)/(q-1)(d,q-1)$, respectively, in the cases $j \le d-2$, $j=d-1$, or $j=d$. A power of w has order $\mathrm{lcm}(r^a,s^b)$.

Next, suppose that $i \nmid j$ and $i+j \le d$; in particular, $i,j \ge 2$ and $i,j \le d-2$. Then $r^a \nmid q^j-1$ (for, since r^a is $\mathrm{lpppd}^{\#}(q;i,d)$ and $(i,j)<i$, we have $r^a \nmid q^{(i,j)}-1$). Similarly, $s^b \nmid q^i-1$. If $r^{a'}=(q^j-1)_r$ and $s^{b'}=(q^i-1)_s$, it follows that $r^{a'}<r^a$ and $s^{b'}<s^b$.

Write $V=V_i \oplus V_j \oplus W_{d-i-j}$ and let $\langle x\rangle \times \langle y\rangle < \mathrm{GL}(d,q)$, where x and y act as Singer cycles (of order q^i-1 and q^j-1) on V_i and V_j, inducing 1 on $V_j \oplus W_{d-i-j}$ and $V_i \oplus W_{d-i-j}$, respectively. Let $x' \in \langle x\rangle$ and $y' \in \langle y\rangle$ have order $r^a s^{b'}$ and $r^{a'}s^b$, respectively. The determinant map $\mathrm{GF}(q^j) \to \mathrm{GF}(q)$ is just the norm map and hence is onto. Since $|\langle y'^{s^b}\rangle| = r^{a'} = (q^j-1)_r$, it follows that $\det\langle y'^{s^b}\rangle$ is the subgroup of order $(q-1)_r$ in $\mathrm{GF}(q)^*$. Thus, there is an integer β such that $(x'y'^{\beta})^{s^b}$ has determinant 1 and order r^a. A similar statement holds if we interchange the roles of r^a and s^b. Hence, some $t \in \langle x',y'\rangle \cap \hat{G}$ has order $r^a s^b$. Since $t|_{V_i}$ and $t|_{V_j}$ have respective orders $r^a s^{b''}$ and $r^{a''}s^b$ for some $a'' \le a'$, $b'' \le b'$, the actions on V_i and V_j of any nontrivial power of t have different orders. Thus, $tZ \in G$ has order $r^a s^b$.

Conversely, suppose that $g \in G$ has order $\mathrm{lcm}(r^a,s^b)$ for an $\mathrm{lpppd}^{\#}(q;i,d)$-number r^a and $\mathrm{lpppd}^{\#}(q;j,d)$-number s^b, where $i \le j$. We have to show that r^a, s^b fall into one of the five cases described in the statement of the proposition. We can suppose that we are not in case (i) or (ii), and hence that either $i+j>d$ or $i=1$, $j=d-1$.

If $h \in \hat{G}$ with $g = hZ$, then V is the direct sum of irreducible $\langle h \rangle$-submodules; moreover, there are summands, $V(i)$ and $V(j)$, on which h induces elements of order divisible by r^a and s^b, respectively. Take a power h^c of h which has order r^a. Then $V(i)$ is the direct sum of irreducible $\langle h^c \rangle$-submodules; since r^a is an lppp$^{\#}(q; i, d)$-number, each of these submodules of $V(i)$ has dimension i by Schur's Lemma. Thus, $i \mid \dim V(i)$. Similarly, $j \mid \dim V(j)$.

We first consider the case $j \neq d - 1$. In particular, $i + j > d$ and hence $j > d/2$ since $j \geq i$. Then $\dim V(i) + \dim V(j) \geq i + j > d$, so $V(i)$ and $V(j)$ must be the same one of our summands. Consequently, $\operatorname{lcm}(i, j) \mid \dim V(i)$, so $\operatorname{lcm}(i, j) \leq d$. Since $j > d/2$ this implies that $i \mid j$. If $j \leq d - 2$ then we are in case (iii). If $j = d$ then we are in case (v), since an element of G acting irreducibly on the natural projective module must have order dividing $(q^d - 1)/(q - 1)(d, q - 1)$.

If $j = d - 1$ then $h \in H := (\langle x \rangle \times \langle y \rangle) \cap \hat{G}$ with $x, y \in \mathrm{GL}(d, q)$, $|x| = q^{d-1} - 1$, and $|y| = q - 1$. As before, for every $x' \in \langle x \rangle$ there is a unique $y_{x'} \in \langle y \rangle$ such that $x' y_{x'} \in H$, so $H = q^{d-1} - 1$. Moreover, $Z \leq H$, since for all $c \in \mathrm{GF}(q)^*$, matrices of the form $\operatorname{diag}(c, c, \ldots, c, c^{1-d})$ occur as matrices of elements of $\langle x^{(q^{d-1}-1)/(q-1)} \rangle$ by using a suitable basis. Hence $|H/Z| = (q^{d-1} - 1)/(d, q - 1)$. Since $g \in H/Z$ we are in case (iv). ∎

Edge types. We shall call an edge in $\Gamma(G)$ connecting r^a and s^b of *type* (z), z $\in$ {i, ii, iii, iv, v}, if it arises as in Proposition 3.3(z). We shall also call the edge in $\Delta(G)$ connecting $\mathbf{C}(r^a)$ and $\mathrm{C}(s^b)$ a *type* (z) *edge*.

PROPOSITION 3.4. *If $i > d/2$ then all* lpppd$^{\#}(q; i, d)$*-numbers are in the same equivalence class in* $\Delta(\mathrm{PSL}(d, q))$.

Proof. For any i, any lpppd$^{\#}(q; i, d)$-numbers s^b, t^c are adjacent by a type (iii), (iv), or (v) edge of $\Gamma(\mathrm{PSL}(d, q))$, and they are adjacent to precisely the same vertices by type (i), (ii), or (iii) edges. If $i \in \{d - 1, d\}$ then s^b and t^c are adjacent to precisely the same vertices by type (iv) or (v) edges. On the other hand, if $d/2 < i \leq d - 2$ then $i \nmid d - 1$ and $i \nmid d$, so neither s^b nor t^c is incident to any type (iv) or (v) edge. ∎

Notation. For $i > d/2$, we shall denote by $C(i)$ the equivalence class containing all lpppd$^{\#}(q; i, d)$-numbers. These are *different classes*. Proposition 3.3 implies that lpppd$^{\#}(q; i, d)$- and lpppd$^{\#}(q; j, d)$-numbers are not adjacent for $d/2 < i < j$.

PROPOSITION 3.5. *Let $d \geq 7$. If r^a is* lpppd$^{\#}(q; i, d)$ *for some $i \geq 4$ then* $v(\mathbf{C}(r^a)) \leq |\Delta(\mathrm{PSL}(d, q))| - 4$.

Proof. For $d-3 \le j \le d$, we have $i+j > d$. Since i can divide at most one of these j, Proposition 3.3 implies that $\mathbf{C}(r^a)$ is neither adjacent nor equal to at least three of these $C(j)$. ∎

PROPOSITION 3.6. *If $d \ge 7$ and r^a is an* lpppd$^{\#}(q; 1, d)$- *or* lpppd$^{\#}(q; 2, d)$*-number, then* $|V(\Delta(\mathrm{PSL}(d, q)))| - 3 \le v(\mathbf{C}(r^a)) \le |V(\Delta(\mathrm{PSL}(d, q)))| - 2$.

Proof. If s^b is an lpppd$^{\#}(q; j, d)$-number for some $j \le d-2$, then $\mathbf{C}(r^a)$ and $\mathbf{C}(s^b)$ are equal or are adjacent by a type (i) or (ii) edge. Hence $v(\mathbf{C}(r^a)) \ge |V(\Delta(\mathrm{PSL}(d, q)))| - 3$. On the other hand, $\mathbf{C}(r^a)$ cannot be adjacent to both $C(d-1)$ and $C(d)$, since r^a cannot divide both of the relatively prime numbers $(q^{d-1}-1)/(d, q-1)$ and $(q^d-1)/(q-1)(d, q-1)$. ∎

PROPOSITION 3.7. *Let $d \ge 7$ and let r^a be an* lpppd$^{\#}(q; 3, d)$*-number. Then $v(\mathbf{C}(r^a)) = |V(\Delta(\mathrm{PSL}(d, q)))| - 3$, with one possible exception; $v(\mathbf{C}(r^a))$ may be $|V(\Delta(\mathrm{PSL}(d, q)))| - 4$ when $3 \mid (q-1, d)$ and $r^a = (q^3-1)_3 = 3(q-1)_3$.*

Proof. By Proposition 3.3(i), (ii), the vertex $\mathbf{C}(r^a)$ is adjacent to every vertex other than $C(d-2), C(d-1), C(d)$, so $v(\mathbf{C}(r^a)) \ge |V(\Delta(\mathrm{PSL}(d, q)))| - 4$.

Since $(q^2+q+1, q-1) = (3, q-1)$ and $9 \nmid q^2+q+1$, and since r is lpppd$^{\#}(q; 3, d)$, either $r \ne 3$ or $r^a = (q^3-1)_3 = 3(q-1)_3$. In the first case, $(r, q-1) = 1$ and $\mathbf{C}(r^a)$ is adjacent to the only vertex $C(j) \in \{C(d-2), C(d-1), C(d)\}$ with $3 \mid j$.

If $r^a = (q^3-1)_3$ then there are two subcases. If $3 \nmid d$ then again $\mathbf{C}(r^a)$ is adjacent by an edge of type (iii) or (iv) to $C(j)$ for the unique $j \in \{d-2, d-1\}$ with $3 \mid j$. Finally, if $3 \mid d$ then $\mathbf{C}((q^3-1)_3)$ may or may not be adjacent to $C(d)$, depending on whether or not $(q^3-1)_3 \mid (q^d-1)/(q-1)(q-1, d)$. ∎

PROPOSITION 3.8. *If $d \ge 7$ then $\Delta(\mathrm{PSL}(d, q))$ has a vertex of valency $|V(\Delta(\mathrm{PSL}(d, q)))| - 2$.*

Proof. If q is not a Mersenne prime then let r be an odd prime divisor of $q+1$. Then r is an lpppd$^{\#}(q; 2, d)$-number, so $\mathbf{C}(r)$ is adjacent to all vertices other than $C(d-1), C(d)$ by type (i) or (ii) edges. Furthermore, $(r, q-1) = 1$, so $\mathbf{C}(r)$ is adjacent to $C(j)$ for even $j \in \{d-1, d\}$ by a type (iv) or (v) edge. Then $v(\mathbf{C}(r)) = |V(\Delta(\mathrm{PSL}(d, q)))| - 2$.

If q is Mersenne then $(q-1)_2(q-1, d)_2 \le 4$ and $8 \mid q^2-1$, so the equivalence class $\mathbf{C}(2)$ of the lpppd$^{\#}(q; 1, d)$-number 2 is adjacent to $C(j)$ for even $j \in \{d-1, d\}$ by a type (iv) or (v) edge. Moreover, $\mathbf{C}(2)$ is adjacent to all vertices other than $C(d-1), C(d)$ by type (i) edges. ∎

PROPOSITION 3.9. *For $d \geq 8$, $\Delta(\mathrm{PSL}(d, q))$ has at least seven vertices.*

Proof. For $3 \leq i \leq d$, let r_i be an $\mathrm{lpppd}^{\#}(q; i, d)$-number relatively prime to $q - 1$. (By Zsigmondy's Theorem, we can choose r_i to be a prime except in the case $q = 2$, $i = 6$, where we use $r_6 = 9$.) We claim that *the vertices $\mathbf{C}(r_i)$ are all different*. If $i, j > d/2$ then $\mathbf{C}(r_i) \neq \mathbf{C}(r_j)$ since r_i and r_j are not adjacent in $\Gamma(\mathrm{PSL}(d, q))$. If $i \leq (d-1)/2$ and $i < j$ then $\mathbf{C}(r_i) \neq \mathbf{C}(r_j)$ since $\mathbf{C}(r_i)$ is adjacent to $\mathbf{C}(r_{d-i})$ by a type (ii) edge and to one of $\mathbf{C}(r_{d-i+1}), \mathbf{C}(r_{d-i+2}), \ldots, \mathbf{C}(r_d)$ by a type (iii), (iv), or (v) edge; however, $\mathbf{C}(r_j)$ is adjacent or equal to at most one of $\mathbf{C}(r_{d-i})$, $\mathbf{C}(r_{d-i+1}), \ldots, \mathbf{C}(r_d)$ (by an edge of type (iii), (iv), or (v)). Finally, if d is even then $\mathbf{C}(r_{d/2}) \neq \mathbf{C}(r_j)$ for $d/2 < j < d$ because $r_{d/2}$ and r_j are not adjacent, and $\mathbf{C}(r_{d/2}) \neq \mathbf{C}(r_d)$ because $r_{d/2}$ is adjacent to $r_{d/2-1}$ (by a type (i) edge) but r_d is not. This proves our claim.

So far we have found $d - 2$ vertices $\mathbf{C}(r_i)$ in $\Delta(\mathrm{PSL}(d, q))$, so we are done if $d \geq 9$. If $d = 8$ then, by Propositions 3.5 and 3.7, all of these vertices $\mathbf{C}(r_i)$ have valency at most $|V(\Delta(\mathrm{PSL}(8, q)))| - 3$. Hence they differ from the vertex of valency $|V(\Delta(\mathrm{PSL}(8, q)))| - 2$ found in Proposition 3.8. ∎

LEMMA 3.10. *If 3^a is an $\mathrm{lpppd}^{\#}(q; i, d)$-number, then $i = 3^m$ or $2 \cdot 3^m$ for some $m \geq 0$.*

Proof. Here q cannot be a power of 3, so $3 \mid q^2 - 1$. Suppose first that i is odd and $i = k \cdot 3^m$ with $3 \nmid k$. Then $3 \mid q^{\mathrm{lcm}(i,2)} - 1 = q - 1$, so $3 \mid q^{3^m} - 1$. By (2.1), $((q^{k3^m} - 1)/(q^{3^m} - 1), q^{3^m} - 1) = (k, q^{3^m} - 1)$, which is not divisible by 3, so $(q^i - 1)_3 = (q^{3^m} - 1)_3$. Since, by definition of $\mathrm{lpppd}^{\#}(q; i, d)$-numbers, $3^a \nmid q^j - 1$ for $1 \leq j < i$, we obtain $k = 1$.

Similarly, if i is even then $i = 2k \cdot 3^m$ with $3 \nmid k$. Then $(q^i - 1)_3 = (q^{2 \cdot 3^m} - 1)_3$ and $k = 1$ as before. ∎

PROPOSITION 3.11. *Let $d \geq 8$ and $i = 3^{m+1}$ or $2 \cdot 3^m$ for some $m \geq 1$. If r^a is an $\mathrm{lpppd}^{\#}(q; i, d)$-number, then $v(\mathbf{C}(r^a)) \leq |V(\Delta(\mathrm{PSL}(d, q)))| - 5$.*

Proof. Since $i > 5$ it can divide at most one of the integers $d - 4, \ldots, d$. Hence, $\mathbf{C}(r^a)$ is different from and not adjacent to at least four of the vertices $\mathbf{C}(r_{d-4}), \mathbf{C}(r_{d-3}), \ldots, \mathbf{C}(r_d)$ defined in the proof of Proposition 3.9. ∎

For $d \leq 7$, we now describe the graphs $\Delta(\mathrm{PSL}(d, q))$ by their adjacency matrices. As usual, the weights of vertices are listed on the left-hand side of the adjacency matrix; the meaning of the numbers on the right-hand side is not needed now, and will be explained in Section 3.2.

The graph $\Delta(\mathrm{PSL}(2,q))$:

$$\begin{matrix}(q-1)/(2,q-1)\\(q+1)/(2,q-1)\end{matrix}\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

The graph $\Delta(\mathrm{PSL}(3,q))$, if $3 \nmid q-1$:

$$\begin{matrix}q^2-1\\q^2+q+1\end{matrix}\begin{pmatrix}0&0\\0&0\end{pmatrix}\begin{matrix}q^2-1\\q^2-q+1\end{matrix}$$

The graph $\Delta(\mathrm{PSL}(3,q))$, if $3 \mid q-1$:

$$\begin{matrix}(q-1)_3\\(q-1)/3*\\(q+1)\cdot(q-1)_2\\(q^2+q+1)/3\end{matrix}\begin{pmatrix}0&1&0&0\\1&0&1&0\\0&1&0&0\\0&0&0&0\end{pmatrix}\begin{matrix}(q+1)_3\\(q+1)/3\\(q-1)\cdot(q+1)_2\\(q^2-q+1)/3\end{matrix}$$

The graph $\Delta(\mathrm{PSL}(4,q))$ (if $q=2$ then vertices $1,5$ do not exist and so vertices 2 and 4 become equivalent):

$$\begin{matrix}(q-1)/(4,q-1)*\\(q+1)\cdot(2,q-1)/(4,q-1)\\(q^2+q+1)\cdot(q-1)_3\\(q^2+1)/(2,q-1)\\(q^2-1)_2*\end{matrix}\begin{pmatrix}0&1&1&0&1\\1&0&0&1&1\\1&0&0&0&0\\0&1&0&0&0\\1&1&0&0&0\end{pmatrix}\begin{matrix}(q+1)/(4,q+1)*\\(q-1)\cdot(2,q-1)/(4,q+1)*\\(q^2-q+1)\cdot(q+1)_3\\(q^2+1)/(2,q-1)\\(q^2-1)_2*\end{matrix}$$

The graph $\Delta(\mathrm{PSL}(5,q))$:

$$\begin{matrix}(q^2+q+1)\cdot(q-1)_3\cdot(q-1)_5\\(q^2-1)/(5,q-1)\\(q^2+1)\cdot(q^2-1)_2\\(q^4+q^3+q^2+q+1)/(5,q-1)\end{matrix}\begin{pmatrix}0&1&0&0\\1&0&1&0\\0&1&0&0\\0&0&0&0\end{pmatrix}\begin{matrix}(q^2-q+1)\cdot(q+1)_3\cdot(q+1)_5\\(q^2-1)/(5,q+1)\\(q^2+1)\cdot(q^2-1)_2\\(q^4-q^3+q^2-q+1)/(5,q+1)\end{matrix}$$

The graph $\Delta(\mathrm{PSL}(6,q))$:

$$\begin{array}{rc|c}
(q-1)/(6,q-1)* & 0\,1\,1\,1\,1\,0\,1 & (q+1)/(6,q+1)* \\
(q+1)/(2,q-1) & 1\,0\,1\,1\,0\,1\,1 & (q-1)/(2,q-1)* \\
(q^2+q+1)/(3,q-1) & 1\,1\,0\,0\,0\,1\,1 & (q^2-q+1)/(3,q+1)* \\
(q^2+1)\cdot(q^2-1)_2 & 1\,1\,0\,0\,0\,0\,1 & (q^2+1)\cdot(q^2-1)_2 \\
(q-1)_5\cdot(q^5-1)/(q-1) & 1\,0\,0\,0\,0\,0\,0 & (q+1)_5\cdot(q^5+1)/(q+1) \\
(q^2-q+1)\cdot(q+1)_3 & 0\,1\,1\,0\,0\,0\,0 & (q^2+q+1)\cdot(q-1)_3 \\
(q^2-1)_2\cdot(q-1)_3* & 1\,1\,1\,1\,0\,0\,1 & (q^2-1)_2\cdot(q+1)_3* \\
(3,q-1)\cdot(q-1)_3* & 1\,1\,1\,0\,0\,0\,1 & (3,q+1)\cdot(q+1)_3*
\end{array}$$

The graph $\Delta(\mathrm{PSL}(7,q))$:

$$\begin{array}{rc|c}
(q^2-1)/(7,q-1) & 0\,1\,1\,1\,1\,0\,1 & (q^2-1)/(7,q+1) \\
(q^2+q+1)\cdot(q-1)_3 & 1\,0\,1\,1\,0\,0\,1 & (q^2-q+1)\cdot(q+1)_3 \\
(q^2-q+1)\cdot(q+1)_3 & 1\,1\,0\,0\,0\,0\,0 & (q^2+q+1)\cdot(q-1)_3 \\
(q^2+1)\cdot(q^2-1)_2 & 1\,1\,0\,0\,0\,0\,1 & (q^2+1)\cdot(q^2-1)_2 \\
(q-1)_5\cdot(q^5-1)/(q-1) & 1\,0\,0\,0\,0\,0\,1 & (q+1)_5\cdot(q^5+1)/(q+1) \\
(q^7-1)/(q-1)(7,q-1) & 0\,0\,0\,0\,0\,0\,0 & (q^7+1)/(q+1)(7,q+1) \\
(q-1)_7* & 1\,1\,0\,1\,1\,0\,0 & (q+1)_7*
\end{array}$$

We now determine the parameters in Definition 2.2:

THEOREM 3.12. *Suppose that* $\Delta(\mathrm{PSL}(d,q))$ *has at least seven vertices. Then* $L_2(G) = (q^2-1)/x$ *for some integer* x, $L_3(G) = (q+1)(q^3-1)$ *or* $(q+1)(q^3-1)/3$, *and* $L(G) = (q+1)(q^3-1)$.

Proof. Suppose first that $d \geq 8$. The least common multiple of all $\mathrm{lpppd}^{\#}(q;1,d)$- and $\mathrm{lpppd}^{\#}(q;2,d)$-numbers is q^2-1, and the least common multiple of all $\mathrm{lpppd}^{\#}(q;i,d)$-numbers for $1 \leq i \leq 3$ is $(q+1)(q^3-1)$. By Propositions 3.5–3.7, the vertices of valency $|V(\Delta(\mathrm{PSL}(d,q)))| - 2$ contain only $\mathrm{lpppd}^{\#}(q;1,d)$- and $\mathrm{lpppd}^{\#}(q;2,d)$-numbers, so $L_2(G) \mid q^2-1$.

By Proposition 3.7, the vertices of valency at least $|V(\Delta(\mathrm{PSL}(d,q)))| - 3$ contain all $\mathrm{lpppd}^{\#}(q;i,d)$-numbers for $1 \leq i \leq 3$—with the possible exception of $3(q-1)_3$— and no $\mathrm{lpppd}^{\#}(q;i,d)$-numbers for $i \geq 4$ by Proposition 3.5. Hence $L_3(G) = (q+1)(q^3-1)$ or $(q+1)/(q^3-1)/3$, as claimed.

Finally, $v(\mathbf{C}(3(q-1)_3)) \geq |V(\Delta(\mathrm{PSL}(d,q)))| - 4$ by Proposition 3.7, while by Proposition 3.10 powers of 3 larger than $3(q-1)_3$ are

lpppd$^{\#}(q; i, d)$-numbers with $i \geq 6$ and hence, by Proposition 3.11, are not involved in the computation of $L(G)$.

If $d \leq 7$ then the proof follows from checking the adjacency matrices given above. For $d \leq 5$, the graph given above has less than seven vertices. For $d = 6$ or 7, if $\Delta(\mathrm{PSL}(d, q))$ has at least seven vertices then the vertex with weight $(q^2 - q + 1) \cdot (q + 1)_3$ has valency at most $|V(\Delta(\mathrm{PSL}(d, q)))| - 5$, so $L(G)$ does not contain a power of 3 not already occurring in $(q + 1)/(q^3 - 1)$. ∎

3.2. PSU(d, q)

We may assume that $d \geq 3$. The isomorphism types of maximal tori in PSU(d, q) can be obtained by replacing q by $-q$ in the cyclic decompositions of maximal tori in PSL(d, q) [Car2]. Hence the graphs $\Delta(\mathrm{PSL}(d, q))$ and $\Delta(\mathrm{PSU}(d, q))$ are closely related, and the weights in $\Delta(\mathrm{PSU}(d, q))$ are obtained by replacing q by $-q$ in the weights of vertices in $\Delta(\mathrm{PSL}(d, q))$. We define *unitary primitive prime power divisor* upppd$^{\#}(q; i, d)$-numbers by replacing q by $-q$ in Definition 3.1. Then analogues of Propositions 3.2–3.7 hold. However, we have to be careful, because for small values of q some of the weights may become 1 and the analogue of Proposition 3.8 is not true for all $d \geq 7$ (for example if $q = 2$ and $3 \mid d$ but $9 \nmid d$).

Edges of *type* (z) refer to the unitary version of Proposition 3.3.

PROPOSITION 3.13. *In each of the following cases,* $\Delta(\mathrm{PSU}(d, q))$ *has a vertex of valency* $|V(\Delta(\mathrm{PSU}(d, q)))| - 2$: (a) $q \geq 4$ *and* $d \geq 4$; (b) $q = 3$ *and* $8 \mid d$; *and* (c) $q = 2$ *and* $d \geq 7$, $3 \nmid d$.

Proof. (a, b) If q is not a Fermat prime then let r be an odd prime divisor of $q - 1$. Since $d \geq 4$, r is a upppd$^{\#}(q; 2, d)$-number, so $\mathbf{C}(r)$ is adjacent to all vertices other than $C(d - 1)$, $C(d)$ by type (i) or (ii) edges. Furthermore, $(r, q + 1) = 1$, so $\mathbf{C}(r)$ is adjacent to $C(j)$ for even $j \in \{d - 1, d\}$ by a type (iv) or (v) edge. Thus, $v(\mathbf{C}(r)) = |V(\Delta(\mathrm{PSU}(d, q)))| - 2$.

If q is Fermat then the equivalence class $\mathbf{C}(2)$ of the upppd$^{\#}(q; 1, d)$-number 2 is adjacent to all vertices other than $C(d - 1), C(d)$ by type (i) edges. If also $q \geq 5$ then $(q + 1)_2(q + 1, d)_2 \leq 4$ and $8 \mid q^2 - 1$, so $\mathbf{C}(2)$ is adjacent to $C(j)$ for even $j \in \{d - 1, d\}$ by a type (iv) or (v) edge.

If $q = 3$ and $8 \mid d$ then $(q + 1)_2(q + 1, d)_2 = 16$ and $32 \mid q^d - 1$, so $\mathbf{C}(2)$ and $C(d)$ are adjacent by a type (v) edge.

(c) If $q = 2$ and $3 \nmid d$ then $\mathbf{C}(3)$ is adjacent to $C(d - 1)$ by a type (iv) edge. Also $\mathbf{C}(3)$ is adjacent to all vertices other than $C(d - 1), C(d)$ by type (i) edges. ∎

Although the proof of Proposition 3.9 depended on Proposition 3.8, the analogue remains valid in the unitary case:

PROPOSITION 3.14. *For $d \geq 8$, $\Delta(\mathrm{PSU}(d,q))$ has at least seven vertices.*

Proof. As in the proof of Proposition 3.9, $\Delta(\mathrm{PSU}(d,q))$ has at least $d-2$ vertices of valency at most $|V(\Delta(\mathrm{PSU}(d,q)))|-3$, so we are done in $d \geq 9$. If $d=8$ then Proposition 3.13 implies that, for all values of q, there is an additional vertex of valency $|V(\Delta(\mathrm{PSU}(d,q)))|-2$. ∎

As mentioned earlier, the graphs $\Delta(\mathrm{PSL}(d,q))$ and $\Delta(\mathrm{PSU}(d,q))$ are closely related, but the weights are different. For $3 \leq d \leq 7$, in Section 3.1 we listed the weights in $\Delta(\mathrm{PSU}(d,q))$ on the right side of the adjacency matrix of $\Delta(\mathrm{PSL}(d,q))$. When $d=3$, the two types of graphs correspond to $3 \mid q+1$ and $3 \nmid q+1$.

Finally, as in the previous section we obtain

THEOREM 3.15. *Suppose that $\Delta(\mathrm{PSU}(d,q))$ has at least seven vertices. Then $L_2(G) = (q^2-1)/x$ for some integer x, $L_3(G) = (q-1)(q^3+1)$ or $(q-1)(q^3+1)/3$, and $L(G) = (q-1)(q^3+1)$. Moreover, if $L_3(G) = (q-1)(q^3+1)/3$ then $3 \mid d$.*

3.3. *PSp*$(2m,q)$

We may suppose that $m \geq 2$. We proceed as in Section 3.1, but this case is simpler since $|Z| \leq 2$.

DEFINITION 3.16. Given integers $1 \leq i \leq m$, we define the notion that a prime power r^a is an $\mathrm{spppd}^{\#}(q; i^+, m)$- or $\mathrm{spppd}^{\#}(q; i^-, m)$-*number* (a *symplectic primitive prime power divisor*):

r^a is an $\mathrm{spppd}^{\#}(q; i^+, m)$-*number* if

- $r^a \mid q^i+1$ if $i < m$ and $r^a \mid (q^i+1)/(2, q-1)$ if $i = m$, but
- $r^a \nmid q^j-1$ and $r^a \nmid q^j+1$ for any $1 \leq j < i$;

r^a is an $\mathrm{spppd}^{\#}(q; i^-, m)$-number if

- $r^a \mid q^i-1$ if $i < m$ and $r^a \mid (q^i-1)/(2, q-1)$ if $i = m$, but
- $r^a \nmid q^j-1$ and $r^a \nmid q^j+1$ for any $1 \leq j < i$.

Note that 2 is both $\mathrm{spppd}^{\#}(q; 1^+, m)$ and $\mathrm{spppd}^{\#}(q; 1^-, m)$ when q is odd, but there are no other ambiguities.

PROPOSITION 3.17. (a) *If q is even then there are no* $\mathrm{spppd}^{\#}(q; 2i^-, m)$-*numbers.*

If q is odd and $(q^2-1)_2 = 2^a$ then 2^{a-k-1} is the only $\mathrm{spppd}^{\#}(q; (2^k)^-, m)$-*number for $2 \leq 2^k < m$; there are no* $\mathrm{spppd}^{\#}(q; 2i^-, m)$-*numbers if $2i$ is not a power of 2 or if $2i = m$.*

(b) *There are* spppd$^{\#}(q; i^{+}, m)$*-numbers for all* $1 \le i \le m$ *as well as* spppd$^{\#}(q; i^{-}, m)$*-numbers for all odd* $1 \le i \le m$*, except that there are no* spppd$^{\#}(2; 1^{-}, m)$*-numbers*.

(c) *If* $i > 1$ *then all* spppd$^{\#}(q; i^{\varepsilon}, m)$*-numbers are odd except when* $i = 2^k$ *and* $\varepsilon = {}^a -$."

Proof. (a) Any odd prime power divisor of $q^{2i} - 1 = (q^i - 1)(q^i + 1)$ must divide one of these two factors. If q is odd then $4 \nmid q^{2j} + 1$ for any j, so for any two odd integers x, y we have $(q^{x2^k} - 1)_2 = (q^{y2^k} - 1)_2$. Hence the spppd powers of 2 occur when $x = 1$.

(b) Zsigmondy's Theorem [Zs] implies the existence of spppd$^{\#}(q; i^{\varepsilon}, m)$-numbers.

(c) If i is odd then $(q^i - 1)_2 = (q - 1)_2$ and $(q^i + 1)_2 = (q + 1)_2$, while if i is even then $(q^i + 1)_2 = (2, q - 1)$. ∎

In the proof of the next two propositions, we shall use the fact that, if $h \in \hat{G}$ is semisimple, then $V = \oplus V(k)$ for irreducible $\langle h \rangle$-submodules $V(k)$ with the following property: each $V(k)$ is either nonsingular and perpendicular to the remaining summands or else is totally isotropic and there is a totally isotropic summand $V(k')$ such that $V(k) \oplus V(k')$ is a nonsingular subspace perpendicular to all other summands. Moreover, if $V(k)$ is totally isotropic then the order of $h|_{V(k)}$ divides $q^{\dim V(k)} - 1$, while if $V(k)$ is nonsingular then the order of $h|_{V(k)}$ divides $q^{\dim V(k)/2} + 1$.

PROPOSITION 3.18. *The vertices of* $\Gamma(\mathrm{PSp}(2m, q))$ *are the* spppd$^{\#}(q; i^{\varepsilon}, m)$*-numbers with* $1 \le i \le m$ *and* $\varepsilon \in \{+, -\}$.

Proof. Suppose that r^a is an spppd$^{\#}(q; i^{\varepsilon}, m)$-number. Write $V = W \perp W^{\perp}$ for a nonsingular $2i$-subspace W. If $\varepsilon =$ "$+$" then consider $x \in \hat{G}$ of order $q^i + 1$, acting irreducibly on W and fixing $W^{\perp}$ pointwise. If $W^{\perp} \neq 0$ then $xZ \in G$ has order $q^i + 1$ and if $W^{\perp} = 0$ then xZ has order $(q^m + 1)/(2, q - 1)$. In both cases, xZ has a power of order r^a. Similarly, if $\varepsilon =$ "$-$" then consider $y \in \hat{G}$ of order $q^i - 1$, acting irreducibly on two complementary i-dimensional totally isotropic subspaces of W while fixing $W^{\perp}$ pointwise, so that some power of yZ has order r^a.

Conversely, suppose that the order of $g \in G$ is a power r^a of a prime $r \neq p$. If $g = hZ$ with $h \in \hat{G}$, then V is the direct sum of irreducible $\langle h \rangle$-modules. Let V_i be one of these summands on which $\langle h \rangle$ acts faithfully, where $i = \dim V_i$. If V_i is nonsingular then i is necessarily even and r^a is an spppd$^{\#}(q; (i/2)^{+}, m)$-number. If V_i is totally isotropic then r^a is an spppd$^{\#}(q; i^{-}, m)$-number or an spppd$^{\#}(q; (i/2)^{-}, m)$-number (the latter case can occur when $r = 2$, $-1 \in \langle h \rangle$, $|h| = 2^{a+1}$, h preserves a decomposition of V into the perpendicular sum of nonsingular subspaces of dimension $2i$ and $2m - 2i$, and yet $|g| = 2^a$ divides $q^{i/2} - 1$). ∎

PROPOSITION 3.19. *Let $m \geq 3$.*

(a) *Let r^a be $\mathrm{spppd}^{\#}(q; i^-, m)$ and let s^b be $\mathrm{spppd}^{\#}(q; j^-, m)$ for some i, j with $1 \leq i \leq j \leq m$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{PSp}(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m$; *or*

(ii) $i \mid j$, *excluding the case in which $i = 1$, $j = m$, q and m are odd, and $r^a = (q-1)_2$.*

(b) *Let r^a be $\mathrm{spppd}^{\#}(q; i^+, m)$ and let s^b be $\mathrm{spppd}^{\#}(q; j^+, m)$ for some i, j with $1 \leq i \leq j \leq m$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{PSp}(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m$;

(ii) $i \mid j$ *with j/i odd, excluding the case in which $i = 1$, $j = m$, q and m are odd, and $r^a = (q+1)_2$.*

(c) *Let r^a be $\mathrm{spppd}^{\#}(q; i^-, m)$ and let s^b be $\mathrm{spppd}^{\#}(q; j^+, m)$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{PSp}(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m$;

(ii) $r = 2$ *and* $1 < j = 2^l < i = 2^k < m$ *for some* k, l;

(iii) m *is odd*, $q \equiv 3 \pmod 4$, $r^a = 2$, $i = 1$, $j = m$; *or*

(iv) m *is odd*, $q \equiv 1 \pmod 4$, $s^b = 2$, $i = m$, $j = 1$.

Proof. We shall use the same argument as in Proposition 3.3.

(a) First we show that, if r^a, s^b satisfy the condition given in the statement of the proposition, then they are adjacent in $\Gamma(\mathrm{PSp}(2m, q))$.

Suppose that $i \mid j$. Write $V = W \perp W^{\perp}$ for a nonsingular $2j$-space W. Let $x \in \hat{G}$ of order $q^j - 1$ act irreducibly on two complementary j-dimensional totally isotropic subspaces of W; some $w \in \langle x \rangle$ has order $\mathrm{lcm}(r^a, s^b)$. If $j < m$ then $\langle x \rangle \cap Z = 1$, so $wZ \in G$ has order $\mathrm{lcm}(r^a, s^b)$. If $j = m$ then m is odd, since there are no $\mathrm{spppd}^{\#}(q; m^-, m)$-numbers for even m (cf. Proposition 3.17(a)). Moreover, s^b is odd since $(q^m - 1)_2 = (q-1)_2$. If r^a is odd then again wZ has order $\mathrm{lcm}(r^a, s^b)$. Finally, if $r^a = 2^a$ then $i = 1$ since $(q^m - 1)_2 = (q-1)_2$. Since we have excluded $r^a = (q-1)_2$, we have $2^{a+1} \mid q - 1$ and hence there is a power x' of x of order $2^{a+1}s^b$, and then $x'Z \in G$ has order $\mathrm{lcm}(r^a, s^b)$.

If $i + j \leq m$ and $i \nmid j$ then, as in the proof of Proposition 3.3, $r^a \nmid q^j - 1$ and $s^b \nmid q^i - 1$. If $s^{b'} = (q^i - 1)_s$ and $r^{a'} = (q^j - 1)_r$, it follows that $s^{b'} < s^b$ and $r^{a'} < r^a$. Let $\langle x \rangle \times \langle y \rangle < \hat{G}$, where x and y act as Singer cycles (of order $q^i - 1$ and $q^j - 1$) on i- and j-dimensional totally isotropic subspaces V_i and V_j of V, respectively, where $V_i \cap V_j = 0$. Let $w \in \langle xy \rangle$ have order $r^a s^b$. Since $w|_{V_i}$ and $w|_{V_j}$ have respective orders $r^a s^{b''}$ and $r^{a''} s^b$

for some $a'' \le a'$, $b'' \le b'$, the actions on V_i and V_j of any nontrivial power of w have different orders. Thus, $wZ \in G$ has order $r^a s^b$.

Conversely, suppose that $g \in g$ has order $\mathrm{lcm}(r^a, s^b)$ for some $\mathrm{spppd}^{\#}(q; i^-, m)$-number r^a and $\mathrm{spppd}^{\#}(q; j^-, m)$-number s^b, with $i \le j$. We may assume that $i + j > m$, in which case we have to show that $i \mid j$ and that we are not in the exceptional case $i = 1$, $j = m$, $r^a = (q-1)_2$.

If $g = hZ$ with $h \in \hat{G}$, then $V = \oplus V(k)$ for irreducible $\langle h \rangle$-submodules $V(k)$. There are summands, $V(i)$ and $V(j)$, on which h induces elements of order divisible by r^a and s^b, respectively. As in the proof of Proposition 3.3, since r^a is an $\mathrm{spppd}^{\#}(q; i^-, m)$-number this implies that $i \mid \dim V(i)$, and similarly $j \mid \dim V(j)$. We claim that $V(i)$ *and* $V(j)$ *are totally isotropic*. For, first note that $s^b > 2$, as otherwise $j = 1$ and $i + j = 2 \le m$, a contradiction. If $V(j)$ is nonsingular then $j \le \dim V(j)/2$ since, by definition, $s^b \nmid q^k + 1$ for $k < j$; however, $(q^j - 1, q^k + 1) = (2, q-1)$ for any $j \le k$, so $s^b \nmid q^{\dim V(j)/2} + 1$, a contradiction. Similarly, if $r^a > 2$ then $V(i)$ is totally isotropic. Finally, $V(i)$ is totally isotropic even in the case $r^a = 2$, since in this case $I + j > m$ implies that $j = m$, so V is the direct sum of two j-dimensional totally isotropic h-invariant subspaces; our decomposition only has two summands, both of which are totally isotropic and one of which must be $V(i)$.

Since $V(i)$ and $V(j)$ are totally isotropic, as noted before Proposition 3.18 there is a summand $V(j')$ such that $W = V(j) + V(j')$ is nonsingular and perpendicular to the remaining summands. Since $\dim V(i) + \dim V(j)$ is larger than the Witt index m of V, $V(i)$ cannot be perpendicular to both $V(j)$ and $V(j')$ and hence must equal one of these. Once again we proceed as in Proposition 3.3: $\mathrm{lcm}(i, j) \mid \dim V(j) = \dim V(j')$, so $\mathrm{lcm}(i, j) \le m$ and hence $i \mid j$ since $j > m/2$. If $j < m$ then we are done. If $j = m$ then m is odd by Proposition 3.17(a), since s^b is an $\mathrm{spppd}^{\#}(q; j^-, m)$-number. The order of h divides $q^m - 1$, and the order of g must divide $(q^m - 1)/(2, q-1)$, so we must exclude the case $r^a = (q-1)_2 > ((q^m - 1)/2)_2$.

(b) The construction of an element of order $\mathrm{lcm}(r^a, s^b)$ is similar to case (a), using elements acting irreducibly on appropriate nonsingular subspaces instead of totally isotropic ones. For the converse, suppose that $g \in G$ has order $\mathrm{lcm}(r^a, s^b)$, where $i \le j$ and $i + j > m$. If $g = hZ$ with $h \in \hat{G}$, then V is a direct sum of $\langle h \rangle$-irreducible submodules; once again let $V(i)$ and $V(j)$ be two of these on which h induces elements of order divisible by r^a and s^b, respectively. If $r^a > 2$ then $2i \mid \dim V(i)$ since r^a is an $\mathrm{spppd}^{\#}(q; i^+, m)$-number; we always have $s^b > 2$, so $2j \mid \dim V(j)$. Suppose first that $r^a > 2$. Then since $2i + 2j > 2m$, our summands $V(i)$ and $V(j)$ must coincide. Moreover, $V(j)$ is nonsingular, since $j > m/2$ and so V has no totally isotropic subspace of dimension at least $2j$. Since $m < \mathrm{lcm}(2i, 2j)$ and $\mathrm{lcm}(2i, 2j) \mid \dim V(j)$, we must have $\dim V(j) = 2j$

and $i \mid j$. Then $h|_{V(j)}$ has cyclic centralizer in $\mathrm{Sp}(V(i))$ of order $q^j + 1$, and hence $r^a \mid (q^i + 1, q^j + 1)$. Now j/i is odd, since otherwise $r^a \mid (q^j - 1, q^j + 1) = (2, q - 1)$ and hence $r^a = 2$, which is not the case. Now suppose that $r^a = 2$. Then $i = 1$, and $i + j > m$ implies that $j = m$. If $m = j/i$ is even then $|g|$, and hence also r^a, divides the odd number $(q^m + 1)/2$. This contradiction shows that j/i is odd. Finally, the case m odd, $r^a = (q + 1)_2$ is excluded as in (a).

(c) The construction of a suitable element of G is similar to cases (a) and (b), so suppose that $g \in G$ has order $\mathrm{lcm}(r^a, s^b)$. We may assume that $i + j > m$. If r^a or s^b is 2 then $\{i, j\} = \{1, m\}$, we are in a situation already considered in (a) or (b), and case (iii) or (iv) occurs in view of the excluded cases in (a)(ii) and (b)(ii).

If $2 \notin \{r^a, s^b\}$ then obtain h, a direct sum decomposition of V, and summands $V(i)$ and $V(j)$ as before. Then $i \mid \dim V(i)$, $2j \mid \dim V(j)$, and $V(i)$ is totally isotropic (since $r^a \neq 2$); define $V(i')$ as before. Since $\dim V(i) + \dim V(i') + \dim V(j) > 2m$ we must have $V(j) \leq V(i) \oplus V(i')$ and hence $V(j) = V(i)$ or $V(i')$. Now $\mathrm{lcm}(2j, i) \mid \dim V(j)$, $2j \leq \dim V(j) \leq m < i + j$, $j < i$ and hence $m < 2i$. Then $\mathrm{lcm}(2j, i) \leq m$ implies that $\mathrm{lcm}(2j, i) = i$. By Proposition 3.17(a), since i is even $r = 2$ and $i = 2^k < m$ for some k, so that $j > m - i \geq 1$ and (ii) holds. ∎

Notation. By Proposition 3.19, for $i \geq 2$ whether an $\mathrm{spppd}^{\#}(q; i^\varepsilon, m)$-number r^a is adjacent to some s^b in $\Gamma(\mathrm{PSp}(2m, q))$ depends on i^ε, not on r^a (note that this is somewhat simpler than the situation in Proposition 3.3). Hence all $\mathrm{spppd}^{\#}(q; i^\varepsilon, m)$-numbers are equivalent, and we shall denote their equivalence class by $C(i^\varepsilon)$. It is possible that $C(i^\varepsilon) = C(j^{\varepsilon'})$ for some $i^\varepsilon \neq j^{\varepsilon'}$ (for example, $C((m/2)^+) = C((m/2)^-)$ if $m \geq 6$ is even and $m/2$ is odd). However, *for all* $i > m/2$ and $j \geq m/2$ *all of the classes* $C(i^-), C(j^+)$ *are different*, since the proposition implies that there is no edge between any pair of the underlying vertices of $\Delta(\mathrm{PSp}(2m, q))$.

PROPOSITION 3.20. *If* $m \geq 5$ *and* $i \geq 3$ *then* $v(C(i^\varepsilon)) \leq |V(\Delta(\mathrm{PSp}(2m, q)))| - 4$.

Proof. Proposition 3.19 implies that $C(i^\varepsilon)$ is different from and not adjacent to at least three of the vertices $C(m^+)$, $C((m-1)^+)$, $C((m-2)^+)$, and $C(j^-)$ with $j \in \{m - 1, m\}$ odd. ∎

PROPOSITION 3.21. *Let* $m \geq 3$. *Then* $v(C(2^-)) \leq |V(\Delta(\mathrm{PSp}(2m, q)))| - 4$.

Proof. We are assuming that $C(2^-)$ exists, in which case q is odd by Proposition 3.17. Proposition 3.19 implies that $C(2^-)$ is not adjacent to $C(m^+)$ and $C((m-1)^+)$, and also not to $C(j^-)$ for odd $j \in \{m - 1, m\}$. We just noted that these vertices are all distinct, since $m - 1 > m/2$. ∎

PROPOSITION 3.22. *When* $m \geq 4$,

$$v(C(2^+)) = \begin{cases} |V(\Delta(\mathrm{PSp}(2m,q)))| - 4 & \text{if } m \equiv 0 \text{ or } 1 \pmod 4, \text{ and} \\ |V(\Delta(\mathrm{PSp}(2m,q)))| - 3 & \text{if } m \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Proof. First note that, if $i \leq m-2$, then $C(2^+)$ is adjacent to or equal to $\mathbf{C}(r^a)$ for all spppd$^{\#}(q; i^{\varepsilon}, m)$-numbers r^a.

If $m \equiv 0 \pmod 4$ then $C(m^-)$ does not exist (by Proposition 3.17(a)) and $C(2^+)$ is not adjacent to $C(m^+)$, $C((m-1)^+)$, and $C((m-1)^-)$.

If $m \equiv 1 \pmod 4$ then $C(2^+)$ is not adjacent to $C(m^+)$, $C((m-1)^+)$, and $C(m^-)$, and it is adjacent to $C((m-1)^-)$ if this vertex exists.

If $m \equiv 2 \pmod 4$ then $C(m^-)$ does not exist, $C(2^+)$ is not adjacent to $C((m-1)^+)$ and $C((m-1)^-)$ but it is adjacent to $C(m^+)$.

If $m \equiv 3 \pmod 4$ then $C(2^+)$ is not adjacent to $C(m^+)$ and $C(m^-)$, and it is adjacent to $C((m-1)^+)$. Moreover, $C((m-1)^-)$ does not exist. ∎

PROPOSITION 3.23. *If* $m \geq 3$ *and* r^a *is an* spppd$^{\#}(q; 1^{\varepsilon}, m)$*-number, then*

$$v(\mathbf{C}(r^a)) = \begin{cases} |V(\Delta(\mathrm{PSp}(2m,q)))| - 3 \\ \qquad \text{for } m, q \text{ odd and } r^a = (q^2-1)_2/2, \text{ and} \\ |V(\Delta(\mathrm{PSp}(2m,q)))| - 2 \qquad \text{otherwise}. \end{cases}$$

Proof. By Proposition 3.19, r^a is adjacent to all spppd$^{\#}(q; j^{\pm}, m)$-numbers with $j \leq m-1$. If m is even then $C(m^-)$ does not exist (by Proposition 3.17), so $C(m^+)$ is the only vertex $\neq \mathbf{C}(r^a)$ not adjacent to $\mathbf{C}(r^a)$.

Suppose that m is odd. If $r^a \mid (q-1)/(2, q-1)$ then $\mathbf{C}(r^a)$ is adjacent to $C(m^-)$ but not to $C(m^+)$; if $r^a \mid (q+1)/(2, q-1)$ then $\mathbf{C}(r^a)$ is adjacent to $C(m^+)$ but not to $C(m^-)$. If, in addition, q is odd, then $r^a = (q^2-1)_2/2$ is also an spppd$^{\#}(q; 1^{\varepsilon}, m)$-number for $q \equiv -\varepsilon 1 \pmod 4$, and $\mathbf{C}(r^a)$ is adjacent to neither $C(m^-)$ nor $C(m^+)$ by Proposition 3.19(a(ii)), (b(ii)). ∎

PROPOSITION 3.24. *If* $m \geq 5$ *then* $\Delta(\mathrm{PSp}(2m,q))$ *has at least seven vertices.*

Proof. By Proposition 3.19, $C(m^+), C((m-1)^+)$, $C((m-2)^+)$, and $C(j^-)$ for odd $j \in \{m-1, m\}$ are four different vertices. If $m = 5$ or $m \geq 7$ then two further vertices are $C((m-3)^+)$ and $C(j^-)$ for odd $j \in \{m-2, m-3\}$. If $m = 6$ then two further vertices are $C(3^+) = C(3^-)$ and $C(2^+)$. In any case, all six vertices mentioned above have valency at

most $|V(\Delta(\mathrm{PSp}(2m,q)))| - 3$, and hence they differ from the vertex of valency $|V(\Delta(\mathrm{PSp}(2m,q)))| - 2$, whose existence was proven in Proposition 3.23. ∎

For $2 \le m \le 4$, we now describe the graphs $\Delta(\mathrm{PSp}(2m,q))$ by their adjacency matrices.

The graph $\Delta(\mathrm{PSp}(4,q))$:

$$\begin{matrix} (q^2-1)/(2,q-1) \\ (q^2+1)/(2,q-1) \end{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

The graph $\Delta(\mathrm{PSp}(6,q))$:

$$\begin{matrix} (q-1)/(2,q-1)* \\ (q+1)/(2,q-1) \\ (q^2+1)/(2,q-1) \\ (q^2-q+1)\cdot(q+1)_3 \\ (q^2+q+1)\cdot(q-1)_3 \\ (q^2-1)_2/(2,q-1)* \\ (q^2-1)_2* \end{matrix} \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The graph $\Delta(\mathrm{PSp}(8,q))$:

$$\begin{matrix} (q^2-1)/(2,q-1) \\ (q^2+1)\cdot(q^2-1)_2/(2,q-1) \\ (q^2-q+1)\cdot(q+1)_3 \\ (q^2+q+1)\cdot(q-1)_3 \\ (q^4+1)/(2,q-1) \end{matrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Once again we can now determine the parameters in Definition 2.2:

THEOREM 3.25. *If $m \ge 3$ then $\Delta(\mathrm{PSp}(2m,q))$ satisfies $L_2(G) > 1$ and one of the following*:

(i) $L_2(G) = (q^2-1)/(2,q-1)^2$ *and* $L_3(G) = (q^2-1)/(2,q-1)$;

(ii) $L_2(G) = (q^2-1)/(2,q-1)^2$ *and* $L_3(G) = (q^4-1)/(2,q-1)^2$;

(iii) $L_2(G) = (q^2-1)/(2,q-1)$ *and* $L_3(G) = (q^4-1)/(2,q-1)^2$; *or*

(iv) $L_2(G) = (q^2-1)/(2,q-1)$ *and* $L_3(G) = (q^2-1)/(2,q-1)$.

Proof. Suppose first that $m \geq 5$. By Propositions 3.20–3.23, if $m \equiv 1 \pmod 4$ then (i) occurs; if $m \equiv 3 \pmod 4$ then (ii) occurs; if $m \equiv 2 \pmod 4$ then (iii) occurs; and if $m \equiv 0 \pmod 4$ then (iv) occurs. The above matrices imply that (i) holds if $m = 3$ while (iv) holds if $m = 4$.

Finally, $L_2(G) > 1$ since $(q^2 - 1)/x = 1$ has no integer solution for q if $x \mid (2, q-1)^2$. ∎

3.4. $\Omega(2m+1, q)$

The isomorphism types of maximal tori in $\Omega(2m+1, q)$ are the same as in $\mathrm{PSp}(2m, q)$ [Car2], so $\Delta(\Omega(2m+1, q)) \cong \Delta(\mathrm{PSp}(2m, q))$.

3.5. $P\Omega^+(2m, q)$

We may suppose that $2m \geq 8$ since $\mathrm{P}\Omega^+(6, q) \cong \mathrm{PSL}(4, q)$ and $\mathrm{P}\Omega^+(4, q)$ is not simple.

DEFINITION 3.26. Given integers $1 \leq i \leq m$, we define the notion that a prime power r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^+, m)$- or $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-*number* (an *o-plus primitive prime power divisor*):

r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^+, m)$-*number* if $i \leq m-1$ and
- $r^a \mid q^i + 1$ but
- $r^a \nmid q^j - 1$ and $r^a \nmid q^j + 1$ for any $1 \leq j < i$;

r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-number if
- $r^a \mid q^i - 1$ if $i < m$ and $r^a \mid (q^i - 1)/(4, q^m - 1)$ if $i = m$, but
- $r^a \nmid q^j - 1$ and $r^a \nmid q^j + 1$ for any $1 \leq j < i$.

As in the symplectic case, if q is odd then 2 is both an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^+, m)$- and an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^-, m)$-number, but there are no other ambiguities.

PROPOSITION 3.27. (a) *If q is even then there are no $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 2i^-, m)$-numbers.*

If q is odd and $(q^2 - 1)_2 = 2^a$ then 2^{a+k-1} is the only $\mathrm{o}^+\mathrm{pppd}^{\#}(q; (2^k)^-; m)$-number for $2 \leq 2^k < m$. Moreover, there are no $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 2i^-, m)$-numbers if $2i$ is not a power of 2 or if $2i = m$.

(b) *There are $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^+, m)$-numbers for all $1 \leq i \leq m-1$.*

There are $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-numbers for all odd $1 \leq i \leq m$, except that there are no $\mathrm{o}^+\mathrm{pppd}^{\#}(2; 1^-, m)$-numbers.

(c) *If $i > 1$ then all $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^\varepsilon, m)$-numbers are odd except when $i = 2^k$ and $\varepsilon =$ "$-$."*

Proof. See the proof of Proposition 3.17. ∎

As in the symplectic case, if $h \in \hat{G}$ is semisimple then $V = \oplus V(k)$ for irreducible $\langle h \rangle$-submodules with the following property: each $V(k)$ is either nonsingular and perpendicular to the remaining summands or else is totally singular and there is a totally singular summand $V(k')$ such that $V(k) \oplus V(k')$ is a nonsingular subspace perpendicular to all other summands. Hence there is a decomposition $V = W_1 \perp \cdots \perp W_l$ such that each W_i is nonsingular and either $h|_{W_i} = 1$, $h|_{W_i} = -1$, $h|_{W_i}$, acts irreducibly on W_i, or there are two complementary $\dim W_i/2$-dimensional totally singular subspaces of W_i on which h acts irreducibly. (This decomposition is not unique because we may split the fixed point space of h and the (-1)-eigenspace of h several ways into the perpendicular sum of subspaces W_i.)

However, there are two new features. One of them is that the number of W_i with non-maximal Witt index is even. The other one is related to the fact that $\hat{G}$ is a *proper* subgroup of $\mathrm{SO}^+(2m, q)$. For each W_i, we have $h|_{W_i} \in \langle x_i|_{W_i} \rangle$, where $x_i \in \mathrm{SO}^+(2m, q)$ has order $q^{\dim W_i/2} + \delta 1$ and is 1 on $W_i^{\perp}$; here $\delta =$ "$-$" if W_i has Witt index $\dim W_i/2$ and $\delta =$ "$+$" otherwise. Then h can be written in the form $h = \prod x_i^{\alpha_i}$. *If q is odd then $\Sigma \alpha_i$ is even* since h has spinor norm 1.

PROPOSITION 3.28. *The vertices of $\Gamma(\mathrm{P}\Omega^+(2m, q))$ are the $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^+, m)$-numbers with $1 \le i \le m - 1$ and the $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-numbers with $1 \le i \le m$.*

Proof. Suppose first that r^a is an *odd* $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^{\varepsilon}, m)$-number. Write $V = W \perp W^{\perp}$ for a nonsingular $2i$-subspace W, of maximal Witt index if $\varepsilon =$ "$-$" and non-maximal Witt index if $\varepsilon =$ "$+$." Consider first the case $\varepsilon =$ "$+$." In this case, $i \le m - 1$ and $W^{\perp} \ne 0$. There exists $x \in \hat{G}$ of order $(q^i + 1)/(2, q - 1)$, acting irreducibly on W and fixing $W^{\perp}$ pointwise. Since $W^{\perp} \ne 0$, $xZ \in G$ also has order $(q^i + 1)/(2, q - 1)$ and some power of xZ has order r^a. Similarly, if $\varepsilon =$ "$-$" then there exists $y \in \hat{G}$ of order $(q^i - 1)/(2, q - 1)$, acting irreducibly on two complementary i-dimensional totally singular subspaces of W and fixing $W^{\perp}$ pointwise. The order of $yZ \in G$ is $(q^i - 1)/(2, q - 1)$ if $i < m$ and $(q^m - 1)/(4, q^m - 1)$ if $i = m$. In both cases, yZ has a power of order r^a.

Now let r^a be an *even* $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^{\varepsilon}, m)$-number. If $i = 1$ then consider a decomposition $V = W_1 \perp W_2 \perp W_3$, where $\dim W_j = 2$ and $|O(W_j)|$ is divisible by $q + \varepsilon 1$ for $j = 1, 2$ (note that ε determines the Witt index of W_j). There exists $x \in \hat{G}$ such that $x|_{W_1}$ and $x|_{W_2}$ have order $q + \varepsilon 1$ and x fixes W_3 pointwise. Since $W_3 \ne 0$, xZ has order $q + \varepsilon 1$ and an appropriate power of xZ has order r^a. If $i > 1$ then $\varepsilon =$ "$-$" and $i = 2^k < m$ for some k (by Proposition 3.27). This time consider a decomposition $V = W_1 \perp W_2 \perp W_3$ such that W_1, W_2, W_3 have maximal Witt index and $\dim W_1 = 2i$, $\dim W_2 = 2$. There exists $x \in \hat{G}$ such that the

order of $x|_{W_1}$ is $q^i - 1$, the order of $x|_{W_2}$ is $q - 1$, and x fixes W_3 pointwise. No nontrivial power of x is in Z, so xZ has order divisible by r^a.

Conversely, suppose that the order of $g \in G$ is a power r^a of a prime $r \neq p$. If $r^a = 2$ then r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^{\varepsilon}, m)$-number for $\varepsilon \in \{+, -\}$, so we may assume that $r^a > 2$. If $g = hZ$ with $h \in \hat{G}$, then V is the direct sum of irreducible $\langle h \rangle$-modules. Let V_i be one of these summands on which $\langle h \rangle$ acts faithfully, where $i = \dim V_i$. If V_i is nonsingular then i is necessarily even and r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; (i/2)^+, m)$-number. If V_i is totally singular then r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-number or $\mathrm{o}^+\mathrm{pppd}^{\#}(q; (i/2)^-, m)$-number (the latter case can occur when $r = 2$, $-1 \in \langle h \rangle$, $|h| = 2^{a+1}$, h preserves a decomposition of V into the perpendicular sum of nonsingular subspaces of dimension $2i$ and $2m - 2i$, and yet $|g| = 2^a$ divides $q^{i/2} - 1$). ∎

PROPOSITION 3.29. *Let $m \geq 4$.*

(a) *Let r^a be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$ and let s^b be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; j^-, m)$ for some i, j with $1 \leq i \leq j \leq m$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{P}\Omega^+(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m$, *or*

(ii) $i \mid j$,

excluding two cases:

(α) $i = 1$, $j = m$, *q and m are odd*, $r^a \nmid (q - 1)/(4, q - 1)$, *and*

(β) $i = 1$, $j = m - 1$, *m is even, and* $r^a = (q - 1)_2$.

(b) *Let r^a be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^+, m)$ and let s^b be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; j^+, m)$ for some i, j with $1 \leq i \leq j \leq m$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{P}\Omega^+(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m$, *or*

(ii) $i \mid j$ *with* $j \mid i$ *is odd*,

excluding two cases:

(α) $i = 1$, $j = m - 1$, *m is odd*, $r^a = 2 = (q + 1)_2$, *and*

(β) $i = 1$, $j = m - 1$, *m is even, and* $r^a = (q + 1)_2$.

(c) *Let r^a be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$ and let s^b be $\mathrm{o}^+\mathrm{pppd}^{\#}(q; j^+, m)$. Then r^a and s^b are adjacent in $\Gamma(\mathrm{P}\Omega^+(2m, q))$ if and only if one of the following holds*:

(i) $i + j \leq m - 1$;

(ii) $r = 2$ *and* $1 \leq j = 2^l < i = 2^k < m$ *for some* k, l;

(iii) $m \equiv 2 \pmod 4$, $i = j = m/2$;

(iv) $q \equiv 3 \pmod 4$, $r^a = 2$, $i = 1$, $j = m - 1$;

(v) m *is odd*, $q \equiv 1 \pmod 8$, $s^b = 2$, $i = m$, $j = 1$; *or*

(vi) m *is even*, $q \equiv 1 \pmod 4$, $s^b = 2$, $i = m - 1$, $j = 1$.

Proof. We shall use the same idea as in Proposition 3.19.

(a) First we show that, if r^a, s^b satisfy the condition given in the statement of the proposition, then they are adjacent in $\Gamma(\mathrm{P}\Omega^+(2m, q))$.

Suppose that $i \mid j$. If $j \leq m - 1$ then write $V = W_1 \perp W_2 \perp W_3$ where W_1 is a nonsingular $2j$-space of Witt index j and W_2 is a nonsingular 2-space of Witt index 1. There exists $x \in \hat{G}$ so that x fixes W_3 pointwise, $x|_{W_1}$ has order $q^j - 1$, acting irreducibly on two complementary j-dimensional totally singular subspaces of W_1, and $x|_{W_2}$ has order $q - 1$, acting irreducibly on two complementary 1-dimensional totally singular subspaces of W_2. Then some $w \in \langle x \rangle$ has order $\mathrm{lcm}(r^a, s^b)$. If moreover $j < m - 1$ then $W_3 \neq 0$ and so $\langle x \rangle \cap Z = 1$; therefore $wZ \in G$ has order $\mathrm{lcm}(r^a, s^b)$. If $j = m - 1$ and m is odd then $s = 2$ and $m - 1 = 2^k$ for some k by Proposition 3.27(a), so that $s^b = (q^{m-1} - 1)_2 > (q - 1)_2$ and again $\langle x \rangle \cap Z = 1$ and $wZ \in G$ has order $\mathrm{lcm}(r^a, s^b)$. If $j = m - 1$ and m is even then s^b is odd. If r^a is also odd then, for $w \in \langle x \rangle$ of order $\mathrm{lcm}(r^a, s^b)$, we have that $wZ \in G$ has order $\mathrm{lcm}(r^a, s^b)$. If r^a is even then $i = 1$, since $i \mid m - 1$ and so i is odd (cf. Proposition 3.27(c)). Since the case $r^a = (q - 1)_2$ is excluded, there is $w \in \langle x \rangle$ of order $\mathrm{lcm}(r^{a+1}, s^b)$ and so $wZ \in G$ has order $\mathrm{lcm}(r^a, s^b)$.

If $j = m$ then m is odd, since there are no $\mathrm{o}^+\mathrm{pppd}^{\#}(q; m^-, m)$-numbers for even m (cf. Proposition 3.27(a)). Moreover, s^b is odd since $(q^m - 1)_2 = (q - 1)_2$. There exists $x \in \hat{G}$ of order $(q^m - 1)/(2, q - 1)$, acting irreducibly on two complementary m-dimensional totally singular subspaces of V, and the order of $xZ \in G$ is $(q^m - 1)/(4, q^m - 1) = (q^m - 1)/(4, q - 1)$. Hence if r^a is odd then a power of xZ has order $\mathrm{lcm}(r^a, s^b)$. Finally, if $r^a = 2^a$ then $i = 1$ since $(q^m - 1)_2 = (q - 1)_2$. Since we have excluded the cases $r^a = (q - 1)_2$ and $r^a = (q - 1)_2/2$, a power of xZ has order $\mathrm{lcm}(r^a, s^b)$.

If $i + j \leq m$ and $i \nmid j$ then, as in the proof of Proposition 3.3, $r^a \nmid q^j - 1$ and $s^b \nmid q^i - 1$. If $s^{b'} = (q^i - 1)_s$ and $r^{a'} = (q^j - 1)_r$, it follows that $s^{b'} < s^b$ and $r^{a'} < r^a$. Write $V = W_1 \perp W_2 \perp W_3$ where W_1 is a nonsingular $2i$-space of Witt index i and W_2 is a nonsingular $2j$-space of Witt index j. Let $x \in \hat{G}$ be such that $x|_{W_1}$ has order $q^i - 1$, $x|_{W_2}$ has order $q^j - 1$, and $x|_{W_3} = 1$. Let $w \in \langle x \rangle$ have order $r^a s^b$. Since $w|_{V_i}$ and $w|_{V_j}$ have respective orders $r^a s^{b''}$ and $r^{a''} s^b$ for some $a'' \leq a'$, $b'' \leq b'$, the actions on W_1 and W_2 of any nontrivial power of w have different orders. Thus, $wZ \in G$ has order $r^a s^b$.

Conversely, suppose that $g \in G$ has order $\mathrm{lcm}(r^a, s^b)$ for some $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^-, m)$-number r^a and $\mathrm{o}^+\mathrm{pppd}^{\#}(q; j^-, m)$-number s^b, with

$i \le j$. We may assume that $i + j > m$ or $i = 1$ and $j = m - 1$, in which cases we have to show that $i \mid j$ and that we are not in the exceptional cases described in (α) and (β).

If $g = hZ$ with $h \in \hat{G}$, then $V = \oplus V(k)$ for irreducible $\langle h \rangle$-submodules $V(k)$. There are summands, $V(i)$ and $V(j)$, on which h induces elements of order divisible by r^a and s^b, respectively. As in the proof of Proposition 3.19, since r^a is an $o^+pppd^{\#}(q; i^-, m)$-number this implies that $i \mid \dim V(i)$, and similarly $j \mid \dim V(j)$. We claim that $V(j)$ *is totally singular*. First we observe that $s^b > 2$, as otherwise $j = 1$ and $i + j = 2 \le m - 1$, a contradiction. If $V(j)$ is nonsingular then $j \le \dim V(j)/2$ since, by definition, $s^b \nmid q^k + 1$ for $k < j$. However, $(q^j - 1, q^k + 1) = (2, q - 1)$ for any $j \le k$, so $s^b \nmid q^{\dim V(j)/2} + 1$, a contradiction. Similarly, if $r^a > 2$ *then* $V(i)$ *is totally singular*.

Since $V(j)$ is totally singular, as noted before Proposition 3.28 there is a summand $V(j')$ such that $W = V(j) + V(j')$ is nonsingular and perpendicular to the remaining summands.

Consider first the case $i + j > m$. If $i = 1$ then obviously $i \mid j$. If $i > 1$ then $r^a > 2$ and $V(i)$ is totally singular. Since $\dim V(i) + \dim V(j)$ is larger than the Witt index m of V, $V(i)$ cannot be perpendicular to both $V(j)$ and $V(j')$ and hence must equal one of these. Once again we proceed as in Proposition 3.19: $\operatorname{lcm}(i, j) \mid \dim V(j) = \dim V(j')$, so $\operatorname{lcm}(i, j) \le m$ and hence $\operatorname{lcm}(i, j) = j$ since $j > m/2$. Hence $i \mid j$ for any value of i. If $j < m$ then we are done. If $j = m$ then m is odd by Proposition 3.27(a), since s^b is an $o^+pppd^{\#}(q; j^-, m)$-number. The order of h divides $(q^m - 1)/(2, q - 1)$, and the order of g must divide $(q^m - 1)/(4, q - 1)$, so we must exclude the case $r^a \nmid (q - 1)/(4, q - 1)$.

If $i = 1$ and $j = m - 1$ then we must show that the case where m is even and $r^a = (q - 1)_2$, described in (β), is impossible. Here $j = m - 1$, $W^{\perp}$ is a 2-dimensional space of maximal witt index, and $W^{\perp}$ is a sum of two 1-dimensional totally singular h-invariant subspaces. There exist $x_1, x_2 \in \mathrm{SO}^+(2m, q)$ such that $x_1|_{W^{\perp}} = 1$, $|x_1| = q^{m-1} - 1$, $x_2|_W = 1$, $|x_2| = q - 1$, and $h \in \langle x_1 \rangle \times \langle x_2 \rangle$. We have $h = x_1^{\alpha_1} x_2^{\alpha_2}$, and one of α_1, α_2 must be odd since $(q^{m-1} - 1)_2 = (q - 1)_2$ must divide $|h|$. However, the spinor norm of h is 1 and so both α_1 and α_2 must be odd. This implies that a power of h is in the center of $\hat{G}$ and so $|g|_2 = (q - 1)_2/2$, a contradiction.

(b) The construction of an element of order $\operatorname{lcm}(r^a, s^b)$ is similar to case (a), using elements acting irreducibly on appropriate nonsingular subspaces instead of totally singular ones. For the converse, suppose that $g \in G$ has order $\operatorname{lcm}(r^a, s^b)$, where $i \le j$ and $i + j > m$ or $i = 1$ and $j = m - 1$. In the first case we have to prove that $i \mid j$ and j/i is odd, while in the second case we have to show that we are not in the exceptional

cases described in (α) and (β). If $g = hZ$ with $h \in \hat{G}$, then V is a direct sum of $\langle h \rangle$-irreducible submodules; once again let $V(i)$ and $V(j)$ be two of these on which h induces elements of order divisible by r^a and s^b, respectively. If $r^a > 2$ then $2i \mid \dim V(i)$ since r^a is an $o^+pppd^{\#}(q; i^+, m)$-number; we always have $s^b > 2$ and so $2j \mid \dim V(j)$.

Consider first the case $i + j > m$. Since there are no $o^+pppd^{\#}(q; m^+, m)$-numbers, we have $j \leq m - 1$, $i \geq 2$ and hence $r^a > 2$. Also, since $2i + 2j > 2m$, our summands $V(i)$ and $V(j)$ must coincide. Moreover, $V(j)$ is nonsingular, since $j > m/2$ and so V has no totally singular subspace of dimension at least $2j$. Since $m < \text{lcm}(2i, 2j)$ and $\text{lcm}(2i, 2j) \mid \dim V(j)$, we must have $\dim V(j) = 2j$ and $i \mid j$. Then $h|_{V(j)}$ has cyclic centralizer in $SO(V(j))$ of order $q^j + 1$, and hence $r^a \mid (q^i + 1, q^j + 1)$. If j/i is even it follows that $r^a \mid (q^j - 1, q^j + 1) = (2, q - 1)$ and hence that $r^a = 2$, which is a contradiction.

Suppose that $i = 1$ and $j = m - 1$. The first subcase we have to exclude is when m is odd and $r^a = 2 = (q + 1)_2$. Suppose that there exists an element of order $\text{lcm}(r^a, s^b)$ in G. Now $V(j)^{\perp}$ is a 2-dimensional space of nonmaximal Witt index. There exist $x_1, x_2 \in SO^+(2m, q)$ such that $x_1|_{V(j)^{\perp}} = 1$, $|x_1| = q^{m-1} + 1$, $x_2|_{V(j)} = 1$, $|x_2| = q + 1$, and $h \in \langle x_1 \rangle \times \langle x_2 \rangle$. We have $h = x_1^{\alpha_1} x_2^{\alpha_2}$, and one of α_1, α_2 must be odd since $(q^{m-1} + 1)_2 = (q + 1)_2 = 2$ must divide $|h|$. However, the spinor norm of h is 1 and so both α_1 and α_2 must be odd. This implies that a power of h is in the center of $\hat{G}$ and so $|g|_2 = (q + 1)_2/2$, a contradiction.

If m is even and $r^a = (q + 1)_2$ then as in the previous paragraph we conclude that there exist $x_1, x_2 \in SO^+(2m, q)$ such that $x_1|_{V(j)^{\perp}} = 1$, $|x_1| = q^{m-1} + 1$, $x_2|_{V(j)} = 1$, $|x_2| = q + 1$, and $h = x_1^{\alpha_1} x_2^{\alpha_2}$. Since $(q^{m-1} + 1)_2 = (q + 1)_2$ holds in this subcase as well, α_1 and α_2 must be odd and a power of h is in the center of $\hat{G}$. So $|g|_2 = (q + 1)_2/2$, which is a contradiction.

(c) The construction of a suitable element of G is similar to cases (a) and (b), so suppose that $g \in G$ has order $\text{lcm}(r^a, s^b)$. We may assume that $i + j \geq m$.

If r^a or s^b is 2 then $\{i, j\} = \{1, m - 1\}$ or $\{i, j\} = \{1, m\}$, we are in a situation already considered in (a) or (b), and one of the cases (iv)–(vi) occurs in view of $(a)(\alpha), (\beta)$ and $(b)(\alpha), (\beta)$.

If $2 \notin \{r^a, s^b\}$ then obtain h, a direct sum decomposition of V, and summands $V(i)$ and $V(j)$ as before. Then $i \mid \dim V(i)$, $2j \mid \dim V(j)$, and $V(i)$ is totally singular (since $r^a, s^b \neq 2$); define $V(i')$ as before. Since $\dim V(i) + \dim V(i') + \dim V(j) \geq 2m$, we must have $V = V(i) \oplus V(i') \oplus V(j)$ or $V(j) \leq V(i) \oplus V(i')$. The first case is impossible since $\dim V(j) = 2j$ forces that $V(j)$ is of non-maximal Witt index and $(V(i) \oplus V(i')) \perp V(j)$ is a decomposition of V with an odd number of components of

non-maximal Witt index, a contradiction. Therefore $V(j) \le V(i) \oplus V(i')$ and hence $V(j) = V(i)$ or $V(i')$. Then $\operatorname{lcm}(2j, i) \mid \dim V(j)$ and $2j \le \dim V(j) \le m \le i + j$; hence $j \le i$ and $m \le 2i$. Now $\operatorname{lcm}(2j, i) \le m$ implies that $\operatorname{lcm}(2j, i) = i$ or $\operatorname{lcm}(2j, i) = 2i = m$. In the first case, since i is even, Proposition 3.27(a) implies that $r = 2$ and $i = 2^k < m$ for some k, and (ii) holds. If $\operatorname{lcm}(2j, i) = 2i = m$ then $i + j \ge m$ implies that $i = j = m/2$ and $V = V(i) \oplus V(i')$ with $\dim V(i) = \dim V(i') = m$. It is impossible that $m/2$ is even, because in that case the only $\mathrm{o}^+\mathrm{pppd}^{\#}(q; (m/2)^-, m)$-number is $r^a = (q^{m/2} - 1)_2 = (q^m - 1)_2/2$. However, $|g|$ divides $(q^m - 1)/(4, q^m - 1) = (q^m - 1)/4$, which is not divisible by $(q^m - 1)_2/2$. Hence we are in case (iii). ∎

Notation. As in the symplectic case, for fixed $i \ge 2$ and $\varepsilon \in \{+, -\}$ all $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^\varepsilon, m)$-numbers are equivalent and we shall denote their equivalence class by $C(i^\varepsilon)$. *For all* $i, j > m/2$, *all of the classes* $C(i^-), C(j^+)$ *are different* since the proposition implies that there is no edge between any pair of the underlying vertices of $\Gamma(\mathrm{P}\Omega^+(2m, q))$.

PROPOSITION 3.30. *If* $m \ge 5$ *and* $i \ge 3$ *then* $v(C(i^\varepsilon)) \le |V(\Delta(\mathrm{P}\Omega^+(2m, q)))| - 4$.

Proof. If $m = 5$ then Propositions 3.27 and 3.29 imply that $C(5^-)$, $C(4^+)$, $C(3^-)$, and $C(3^+)$ are four different, pairwise nonadjacent vertices, and $C(i^\varepsilon)$ is different from and not adjacent to at least three of these. If $m = 6$ then $C(5^+)$, $C(5^-)$, $C(4^+)$, and $C(3^+)$ are four different, pairwise nonadjacent vertices, and $C(i^\varepsilon)$ is different from and not adjacent to at least three of these. If $m \ge 7$ then $C((m-1)^+)$, $C((m-2)^+)$, $C((m-3)^+)$, and $C(j^-)$ with $m - 3 \le j \le m$ odd are five different, pairwise nonadjacent vertices; once again $C(i^\varepsilon)$ is different from and not adjacent to at least three of them. ∎

PROPOSITION 3.31. *Let* $m \ge 4$. *Then* $v(C(2^-)) \le |V(\Delta(\mathrm{P}\Omega^+(2m, q)))| - 4$.

Proof. We are assuming that $C(2^-)$ exists, in which case q is odd. Proposition 3.29(c) implies that $C(2^-)$ is not adjacent to $C((m-1)^+)$ and $C((m-2)^+)$, and also not to $C(j^-)$ for odd $j \in \{m-1, m\}$. ∎

PROPOSITION 3.32. *If* $m \ge 5$, *then*

$$v(C(2^+)) = \begin{cases} |V(\Delta(\mathrm{P}\Omega^+(2m, q)))| - 4 & \text{if } m \equiv 1 \pmod 4, \text{ and} \\ |V(\Delta(\mathrm{P}\Omega^+(2m, q)))| - 3 & \text{otherwise.} \end{cases}$$

Proof. $C(2^+)$ is adjacent to or equal to $\mathbf{C}(r^a)$ for all $\mathrm{o}^+\mathrm{pppd}^{\#}(q; i^\varepsilon, m)$-numbers r^a, where $i \le m - 3$ in the case $\varepsilon =$ "$-$" and

$i \le m-2$ in the case $\varepsilon =$ "+." It remains to consider the vertices $C((m-2)^-)$, $C((m-1)^\varepsilon)$, and $C(m^-)$ (recall that $C(m^+)$ does not exist by Proposition 3.27).

If m is even then $C(2^+)$ is not adjacent to $C((m-1)^+)$ and $C((m-1)^-)$, and it is adjacent to $C((m-2)^-)$ by an edge of type (c(ii)) if this vertex exists. Note that $C(m^-)$ does not exist by Proposition 3.27(a).

If $m \equiv 3 \pmod 4$ then $C(2^+)$ is not adjacent to $C(m^-)$ and $C((m-2)^-)$, and it is adjacent to $C((m-1)^+)$. Note that $C((m-1)^-)$ does not exist by Proposition 3.27(a).

If $m \equiv 1 \pmod 4$ then $C(2^+)$ is not adjacent to $C(m^-), C((m-2)^-)$, and $C((m-1)^+)$. It is adjacent to $C((m-1)^-)$ by an edge of type (c(ii)) if this latter vertex exists. ∎

PROPOSITION 3.33. *If $m \ge 4$ is even and r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^\varepsilon, m)$-number, then*

$$v(\mathbf{C}(r^a)) = \begin{cases} |V(\Delta(\mathrm{P}\Omega^+(2m,q)))| - 3 \\ \quad \text{for } q \text{ odd and } r^a = (q^2-1)_2/2, \text{ and} \\ |V(\Delta(\mathrm{P}\Omega^+(2m,q)))| - 2 \quad \text{otherwise}. \end{cases}$$

Proof. If $r^a \mid (q-1)/(2, q-1)$ then the only vertex not adjacent to $\mathbf{C}(r^a)$ is $C((m-1)^+)$. If $r^a \mid (q+1)/(2, q-1)$ then $\mathbf{C}(r^a)$ is adjacent to all vertices except $C((m-1)^-)$. (Note that edges of type (c(iii)), (c(v)) cannot occur here.)

The only $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^\varepsilon, m)$-number not dividing $(q-1)/(2, q-1)$ or $(q+1)/(2, q-1)$ is $(q^2-1)_2/2$ for q odd; it is adjacent to all vertices except $C((m-1)^-)$ and $C((m-1)^+)$. ∎

PROPOSITION 3.34. *Suppose that $m \ge 5$ is odd and r^a is an $\mathrm{o}^+\mathrm{pppd}^{\#}(q; 1^\varepsilon, m)$-number.*

(a) *If q is even or $q \equiv 3 \pmod 4$, then $v(\mathbf{C}(r^a)) = |V(\Delta(\mathrm{P}\Omega^+(2m,q)))| - 2$.*

(b) *When $q \equiv 1 \pmod 4$,*

$$v(\mathbf{C}(r^a)) = \begin{cases} |V(\Delta(\mathrm{P}\Omega^+(2m,q)))| - 2 \\ \quad \text{if } r^a \mid (q-1)/4 \quad \text{or} \quad r^a \mid (q+1)/2, \text{ and} \\ |V(\Delta(\mathrm{P}\Omega^+(2m,q)))| - 3 \\ \quad \text{if } r^a \in \{(q-1)_2, (q-1)_2/2\}. \end{cases}$$

Proof. (a) If $r^a \mid (q-1)/(2, q-1)$ then $\mathbf{C}(r^a)$ is adjacent to all vertices except $C((m-1)^+)$. If $r^a \mid q+1$ then $\mathbf{C}(r^a)$ is adjacent to all vertices except $C(m^-)$ (since m is odd).

(b) If $r^a \mid (q-1)/4$ then $\mathbf{C}(r^a)$ is adjacent to all vertices except $C((m-1)^+)$. If $r^a \mid (q+1)/2$ then $\mathbf{C}(r^a)$ is adjacent to all vertices except $C(m^-)$.

The only $o^+pppd^\#(q; 1^\varepsilon, m)$-numbers not dividing $(q-1)/4$ or $(q+1)/2$ are $(q-1)_2$ and $(q-1)_2/2$; their equivalence class is adjacent to all vertices except $C((m-1)^+)$ and $C(m^-)$. ∎

PROPOSITION 3.35. *If $m \geq 5$ and q is odd, or if $m \geq 7$, then $\Delta(P\Omega^+(2m, q))$ has at least seven vertices.*

Proof. If $m \geq 8$ then there are at least six pairwise nonadjacent vertices $C(i^\varepsilon)$ with $i \geq m/2$. By Proposition 3.30, all of these have valence $\leq |V(\Delta(P\Omega^+(2m, q)))| - 4$, and hence they must differ from the vertex $\mathbf{C}(r^a)$ considered in Propositions 3.33 and 3.34.

If $m = 7$ then $C(7^-)$, $C(6^+)$, $C(5^+)$, $C(5^-)$, $C(4^+)$ are five pairwise nonadjacent vertices, $C(2^+)$ is different from these because $v(C(2^+)) = |V(\Delta(P\Omega^+(14, q)))| - 3$ by Proposition 3.32, and there is a vertex of valency $|V(\Delta(P\Omega^+(14, q)))| - 2$ by Proposition 3.34.

Finally, if $5 \leq m \leq 6$ and q is odd then there are exactly seven vertices $C(i^\varepsilon)$ with $i \geq 2$ and $\varepsilon \in \{+, -\}$ (note that $C(3^+) = C(3^-)$ when $m = 6$). ∎

The graph $\Delta(P\Omega^+(8, q))$ is isomorphic to $\Delta(PSp(6, q))$.

The graph $\Delta(P\Omega^+(10, q))$ when q is even:

$$\begin{array}{r} q-1* \\ q+1 \\ (q^2+1)(q^2-q+1)\cdot(q+1)_3 \\ (q^2+q+1)\cdot(q-1)_3 \\ q^4+1 \\ (q^4+q^3+q^2+q+1)\cdot(q-1)_5 \end{array} \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The graph $\Delta(P\Omega^+(12, q))$ when q is even:

$$\begin{array}{r} q-1* \\ q+1 \\ q^2+1 \\ (q^4+q^2+1)\cdot(q^2-1)_3 \\ q^4+1 \\ (q^4-q^3+q^2-q+1)\cdot(q+1)_5 \\ (q^4+q^3+q^2+q+1)\cdot(q-1)_5 \end{array} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

THEOREM 3.36. *If* $m \geq 4$ *then* $L_2(G) > 1$, *and one of the following occurs in* $\Delta(\mathrm{P}\Omega^+(2m, q))$:

(i) $L_2(G) = (q^2 - 1)/(2, q - 1)^3$ *and* $L_3(G) = (q^2 - 1)/(2, q - 1)$;

(ii) $L_2(G) = (q^2 - 1)/(2, q - 1)^2$ *and* $L_3(G) = (q^4 - 1)/(2, q - 1)^2$;

(iii) $L_2(G) = (q^2 - 1)/(2, q - 1)$ *and* $L_3(G) = (q^4 - 1)/(2, q - 1)^2$;

(iv) $L_2(G) = (q^2 - 1)/(2, q - 1)$ *and* $L_3(G) = (q^2 - 1)/(2, q - 1)$; *or*

(v) $L_2(G) = (q^2 - 1)/(2, q - 1)^3$ *and* $L_3(G) = (q^4 - 1)/(2, q - 1)^2$.

Proof. By Propositions 3.30–3.34,

$m \equiv 1 \pmod 4$	and	$q \equiv 1 \pmod 4$	$\Rightarrow$	(i)
$m \equiv 3 \pmod 4$	and	$q \equiv 3 \pmod 4$	$\Rightarrow$	(iii)
$m \equiv 1 \pmod 4$	and	$q \equiv 3 \pmod 4$	$\Rightarrow$	(iv)
$m \equiv 3 \pmod 4$	and	$q \equiv 1 \pmod 4$	$\Rightarrow$	(v)
m even	and	q odd	$\Rightarrow$	(ii).

If q is even then cases (i), (iv) coincide and occur when $m \equiv 1 \pmod 4$. Cases (ii), (iii), (iv) also coincide and occur when m is even or $m \equiv 3 \pmod 4$.

If $q = 3$ then we are in one of the cases (ii)–(iv), and $L_2(G) > 1$. For all other values of q, we have $L_2(G) > 1$ in (i)–(v). ∎

3.6. $\mathrm{P}\Omega^-(2m, q)$

We may suppose that $m \geq 4$ since $\mathrm{P}\Omega^-(6, q) \cong \mathrm{PSU}(4, q)$ and $\mathrm{P}\Omega^-(4, q) \cong \mathrm{PSL}(4, q^2)$. Although we cannot proceed as simply as in Section 3.2, where results for special linear groups were easily transformed into ones for unitary groups, nevertheless the results and proofs in this section are very similar to the case $\mathrm{P}\Omega^+(2m, q)$ discussed in Section 3.5. We state the usual sequence of propositions, but the proofs are omitted.

DEFINITION 3.37. Given integers $1 \leq i \leq m$, we define the notion that a prime power r^a is an $\mathrm{o}^-\mathrm{pppd}^{\#}(q; i^+, m)$- or $\mathrm{o}^-\mathrm{pppd}^{\#}(q; i^-, m)$-*number* (an *o-minus primitive prime power divisor*):

r^a is an $\mathrm{o}^-\mathrm{pppd}^{\#}(q; i^+, m)$-*number* if $i \leq m$,

- $r^a \mid q^i + 1$ if $i < m$ and $r^a \mid (q^i + 1)/(4, q^m + 1)$ if $i = m$, but
- $r^a \nmid q^j - 1$ and $r^a \nmid q^j + 1$ for any $1 \leq j < i$;

r^a is an $\mathrm{o}^-\mathrm{pppd}^{\#}(q; i^-, m)$-number if $i < m$ and

- $r^a \mid q^i - 1$, but
- $r^a \nmid q^j - 1$ and $r^a \nmid q^j + 1$ for any $1 \le j < i$.

PROPOSITION 3.38. (a) *If q is even then there are no* $o^-pppd^\#(q; 2i^-, m)$*-numbers.*

If q is odd and $(q^2 - 1)_2 = 2^a$ then 2^{a+k-1} is the only $o^-pppd^\#(q; (2^k)^-, m)$*-number for $2 \le 2^k < m$; there are no* $o^-pppd^\#(q; 2i^-, m)$*-numbers if $2i$ is not a power of 2.*

(b) *There are* $o^-pppd^\#(q; i^+, m)$*-numbers whenever $1 \le i \le m$ and* $o^-pppd^\#(q; i^-, m)$*-numbers for all odd $1 \le i \le m - 1$, except that there are no* $o^-pppd^\#(2; 1^-, m)$*-numbers.*

(c) *If $i > 1$ then all* $o^-pppd^\#(q; i^\varepsilon, m)$*-numbers are odd except when $i = 2^k$ and $\varepsilon =$ "$-$."*

PROPOSITION 3.39. *The vertices of $\Gamma(P\Omega^-(2m, q))$ are the* $o^-pppd^\#(q; i^+, m)$*-numbers with $1 \le i \le m$ and the* $o^-pppd^\#(q; i^-, m)$*-numbers with $1 \le i \le m - 1$.*

PROPOSITION 3.40. *Let $m \ge 4$.*

(a) *Let r^a be* $o^-pppd^\#(q; i^-, m)$ *and let s^b be* $o^-pppd^\#(q; j^-, m)$ *for some $1 \le i \le j \le m - 1$. Then r^a and s^b are adjacent in $\Gamma(P\Omega^-(2m, q))$ if and only if one of the following holds*:

(i) $i + j \le m - 1$; *or*

(ii) $i \mid j$.

(b) *Let r^a be* $o^-pppd^\#(q; i^+, m)$ *and let s^b be* $o^-pppd^\#(q; j^+, m)$ *for some $1 \le i \le j \le m$. Then r^a and s^b are adjacent in $\Gamma(P\Omega^-(2m, q))$ if and only if one of the following holds*:

(i) $i + j \le m - 1$; *or*

(ii) $i \mid j$ *with j/i is odd, excluding the case in which $i = 1$, $j = m$, both m and q are odd, $r = 2$, and $r^a \nmid (q + 1)/(4, q + 1)$.*

(c) *Let r^a be* $o^-pppd^\#(q; i^-, m)$ *and let s^b be* $o^-pppd^\#(q; j^+, m)$. *Then r^a and s^b are adjacent in $\Gamma(P\Omega^-(2m, q))$ if and only if one of the following holds*:

(i) $i + j \le m$, *excluding the case in which $i = 1$, $j = m - 1$, m is odd, $q \equiv 3 \pmod 4$, and $r^a = 2$;*

(ii) $r = 2$ *and $1 \le j = 2^l < i = 2^k < m$ for some k, l; or*

(iii) m *is odd, $q \equiv 7 \pmod 8$, $r^a = 2$, $i = 1$, $j = m$.*

Notation. For $i \ge 2$ define the equivalence class $C(i^\varepsilon)$ as before. *For all $i, j > m/2$, all of the classes $C(i^-), C(j^+)$ are different.*

PROPOSITION 3.41. *If $m \ge 5$ and $i \ge 3$ then $v(C(i^\varepsilon)) \le |V(\Delta(P\Omega^-(2m, q)))| - 4$.*

PROPOSITION 3.42. *If $m \geq 4$ then $v(C(2^-)) \leq |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 4$.*

PROPOSITION 3.43. *When $m \geq 4$,*

$$v(C(2^+)) = \begin{cases} |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 3 & \text{if } m \equiv 3 \pmod 4, \text{ and} \\ |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 4 & \text{otherwise.} \end{cases}$$

PROPOSITION 3.44. *Let $m \geq 4$ be even and let r^a be an $\mathrm{o}^-\mathrm{pppd}^{\#}(q; 1^\varepsilon, m)$-number. Then $v(\mathbf{C}(r^a)) = |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 2$.*

PROPOSITION 3.45. *Suppose that $m \geq 5$ in odd and r^a is an $\mathrm{o}^-\mathrm{pppd}^{\#}(q; 1^\varepsilon, m)$-number.*

(a) *If q is even or $q \equiv 1 \pmod 4$, then $v(\mathbf{C}(r^a)) = |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 2$.*

(b) *When $q \equiv 3 \pmod 4$,*

$$v(\mathbf{C}(r^a)) = \begin{cases} |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 2 \\ \quad \text{if } r^a \mid (q+1)/4 \text{ or } r^a \mid (q-1)/2, \text{ and} \\ |V(\Delta(\mathrm{P}\Omega^-(2m,q)))| - 3 \\ \quad \text{if } r^a \in \{(q+1)_2, (q+1)_2/2\}. \end{cases}$$

PROPOSITION 3.46. *If $m = 5$ and q is odd, or if $m \geq 6$, then $\Delta(\mathrm{P}\Omega^-(2m,q))$ has at least seven vertices.*

The graph $\Delta(\mathrm{P}\Omega^-(8,q))$ is isomorphic to $\Delta(\mathrm{PSp}(8,q))$.

The graph $\Delta(\mathrm{P}\Omega^-(10,q))$ when q is even:

$$\begin{array}{r} q-1* \\ q+1 \\ (q^2+1)(q^2+q+1)\cdot(q-1)_3 \\ (q^2-q+1)\cdot(q+1)_3 \\ q^4+1 \\ (q^4-q^3+q^2-q+1)\cdot(q+1)_5 \end{array} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

THEOREM 3.47. *If $m \geq 4$ then one of the following occurs in $\Delta(\mathrm{P}\Omega^-(2m,q))$:*

(i) *$L_2(G) = (q^2-1)/(2, q-1)^3$ and $L_3(G) = (q^2-1)/(2, q-1)$;*

(ii) *$L_2(G) = (q^2-1)/(2, q-1)$ and $L_3(G) = (q^2-1)/(2, q-1)$;*

(iii) $L_2(G) = (q^2 - 1)/(2, q - 1)$ *and* $L_3(G) = (q^4 - 1)/(2, q - 1)^2$; *or*

(iv) $L_2(G) = (q^2 - 1)/(2, q - 1)^3$ *and* $L_3(G) = (q^4 - 1)/(2, q - 1)^2$.

Moreover $L_2(G) > 1$ *unless* $q = 3$ *and* m *is odd.*

Proof. By Propositions 3.41–3.45,

$m \equiv 1 \pmod 4$	and	$q \equiv 3 \pmod 4$	$\Rightarrow$	(i)
$m \equiv 1 \pmod 4$	and	$q \equiv 1 \pmod 4$	$\Rightarrow$	(ii)
$m \equiv 3 \pmod 4$	and	$q \equiv 1 \pmod 4$	$\Rightarrow$	(iii)
$m \equiv 3 \pmod 4$	and	$q \equiv 3 \pmod 4$	$\Rightarrow$	(iv)
m even	and	q odd	$\Rightarrow$	(ii).

If q is even then cases (i), (ii) coincide and occur when m is even or $m \equiv 1 \pmod 4$. Cases (iii), (iv) also coincide and occur when $m \equiv 3 \pmod 4$.

If $q \neq 3$ then $L_2(G) > 1$ in (i)–(iv). If $q = 3$ then $L_2(G) = 1$ if and only if we are in case (i) or (iv), and these cases occur precisely when m is odd. ∎

4. PROOF OF THEOREM 1.1

We have to prove that, with the exceptions listed in Theorem 1.1, $\Delta(G)$ determines G. For the graph parameters $L_2(G), L_3(G), L(G)$, see Definition 2.2. We distinguish three cases:

Case I. $|V(\Delta(G))| \geq 7$ and $L_2(G) > 1$.

Case II. $|V(\Delta(G))| \geq 7$ and $L_2(G) = 1$.

Case III. $|V(\Delta(G))| \leq 6$.

4.1. *Case I*

The only exceptional group belonging to this case is $F_4(q)$ with q odd, while most classical groups belong here.

PROPOSITION 4.1. *If* $G \cong F_4(t)$ *for some odd* t *and* G^* *is a classical simple group, then* $\Delta(G) \ncong \Delta(G^*)$.

Proof. Suppose that $\Delta(G) \cong \Delta(G^*)$, where G^* is defined over GF(q). Then, in particular, the value of $L(G)$ is the same in both graphs. Suppose first that G^* is a special linear or unitary group. By inspecting the adjacency matrix of $\Delta(F_4(t))$ in Section 2.6 and by Theorems 3.12, 3.15, we have $t^2 - 1 = L(G) = L(G^*) = (q \pm 1)(q^3 \mp 1)$. So $t^2 = q(q^3 \pm q^2 \mp 1)$,

which is a contradiction, since the left-hand side is a prime power and the right-hand side is the product of two relatively prime numbers.

Suppose now that G^* is a symplectic or orthogonal simple group. This time, we compare the values of $L_2(G)$ and $L_3(G)$. We have $L_2(G) = 2$. By Theorems 3.25, 3.36, 3.47 and Section 3.4, we have $L_2(G^*) = (q^2 - 1)/x$ for some $x \in \{1, 2, 4, 8\}$. The only possibility for $L_2(G) = L_2(G^*)$ is that $x = 4$ and $q = 3$. However, we get a contradiction even in this case: $t^2 - 1 = L_3(G) = L_3(G^*) = (3^2 - 1)/2$ or $(3^4 - 1)/4$, and these equations have no solution for an integer t. ∎

Proposition 4.1 implies that $\Delta(F_4(q))$ with q odd is not isomorphic to the graph of any classical group. The value of $L(F_4(q)) = q^2 - 1$ also uniquely determines the size of the underlying field, as required in Theorem 1.1.

PROPOSITION 4.2. *Let G be a special linear or unitary simple group, and let G^* be a symplectic or orthogonal simple group. If $|V(\Delta(G))| \geq 7$ then $\Delta(G) \ncong \Delta(G^*)$.*

Proof. Suppose that G is defined over GF(t), G^* is defined over GF(q), and $\Delta(G) \cong \Delta(G^*)$. By Theorems 3.25, 3.36, 3.47 and Section 3.4, $L_3(G^*)$ can be expressed as a function of $L_2(G^*)$ using one of the seven functions

$$\begin{aligned} &f_1: y \mapsto y, && f_4: y \mapsto y(y+1), \\ &f_2: y \mapsto 2y, && f_5: y \mapsto 2y(2y+1), && f_7: y \mapsto y(y+2). \\ &f_3: y \mapsto 4y, && f_6: y \mapsto 4y(4y+1), \end{aligned} \tag{4.3}$$

(The functions $f_1, \ldots, f_6$ occur for odd q and f_1, f_7 occur for even q.)

By Theorems 3.12 and 3.15, $L_2(G) = (t^2 - 1)/x$ and $L_3(G) = (t \pm 1)(t^3 \mp 1)$ or $(t \pm 1)(t^3 \mp 1)/3$. We shall prove that $f(L_2(G)) = L_3(G)$ is impossible, using any of the seven functions f listed above. If $x \geq 10$ then

$$\begin{aligned} f\big(L_2(G)\big) &\leq 4L_2(G)\big(4L_2(G) + 1\big) \\ &\leq \frac{4(t^2-1)}{10}\left(\frac{4(t^2-1)}{10} + 1\right) < (t^2-1)\frac{t^2 - t + 1}{3} \\ &\leq L_3(G). \end{aligned}$$

If $1 \leq x \leq 9$ then we consider $252 = 9 \cdot 4 \cdot 7$ cases (nine possibilities for x, four for $L_3(G)$, and seven for f). In each case, we get a quadratic equation for t. There are five cases when we get an integer solution $t > 1$ for these equations:

(i) $t = 2$, $x = 1$, $L_3(G) = (t - 1)(t^3 + 1)/3 = f_1(L_2(G))$;

(ii) $t = 2$, $x = 2$, $L_3(G) = (t - 1)(t^3 + 1)/3 = f_2(L_2(G))$;

(iii) $t = 2$, $x = 4$, $L_3(G) = (t-1)(t^3+1)/3 = f_3(L_2(G))$;
(iv) $t = 2$, $x = 3$, $L_3(G) = (t-1)(t^3+1)/3 = f_7(L_2(G))$; and
(v) $t = 5$, $x = 2$, $L_3(G) = (t-1)(t^3+1)/3 = f_7(L_2(G))$.

Cases (ii), (iii) are eliminated because $L_2(G) = (t^2-1)/x$ is not an integer, and case (iv) is impossible since $L_2(G) = 1$ cannot occur in Case I. In case (v) we get $L_2(G^*) = 12$, and q must be even (since f_7 occurs only for even q), and then $L_2(G^*) = q^2 - 1 = 12$ has no integer solution.

Eliminating case (i) requires more work. In this case, we have $L_3(G) = 3 = (t-1)(t^3+1)/3$, which implies that $G \cong \mathrm{PSU}(d,2)$ for some d (since $L_3(G) = (t+1)(t^3-1)$ in special linear groups), and moreover, $3 \mid d$ by Theorem 3.15. Since, PSU(3, 2) is not simple, we have $d \geq 6$. We also have $L_2(G^*) = 3 = (q^2-1)/z$, with $z = 1$ if q is even and $z = 2$ if q is odd (cf. Theorems 3.25(iv), 3.36(iv) and 3.47(ii)). This implies $q = 2$.

We claim that *the weights in* $\Delta(\mathrm{PSU}(d,2))$, $d \geq 5$, *cannot be equal to the weights in the graph of any symplectic or orthogonal group defined over* GF(2) (i.e., these graphs can be distinguished even without looking at the edges). Note that for $i > d$, the $\mathrm{ppd}^{\#}(2;i)$-numbers dividing the weights in $\Delta(\mathrm{PSU}(d,2))$ are $\mathrm{ppd}^{\#}(2;2j)$-numbers for odd $j \leq d$ (cf. Section 3.1). Hence, for the largest k such that a $\mathrm{ppd}^{\#}(2;k)$-number divides some weight in $\Delta(\mathrm{PSU}(d,2))$, we have $k = 2j$ for odd $j \in \{d-1, d\}$. Also, since $d \geq 5$, $k - 2 \geq 2(d-1) - 2 > d$, so no $\mathrm{ppd}^{\#}(2;k-2)$-number divides any weight in $\Delta(\mathrm{PSU}(d,2))$. On the other hand, if $k \geq 10$ is the largest integer such that a $\mathrm{ppd}^{\#}(2;k)$-number divides some weight in a symplectic or orthogonal simple group G^* defined over GF(2), then $G^* \cong \mathrm{PSp}(2k,2)$, $\mathrm{P\Omega}^-(2k,2)$, or $\mathrm{P\Omega}^+(2k+2,2)$. In any of these groups, there are $\mathrm{ppd}^{\#}(2;k-2)$-numbers dividing some weight in $\Delta(G^*)$. This distinguishes the unitary situation from the symplectic and orthogonal ones. ▮

PROPOSITION 4.4. *If G is a special linear and G^* is a unitary simple group belonging to Case I, then* $\Delta(G) \not\cong \Delta(G^*)$.

Proof. Suppose that G is defined over GF(t), G^* is defined over GF(q), and $\Delta(G) \cong \Delta(G^*)$. By Theorems 3.12 and 3.15, $L(G) = (t+1)(t^3-1) = (q-1)(q^3+1) = L(G^*)$. This is a contradiction, since the functions $f(n) = (n+1)(n^3-1)$ and $g(n) = (n-1)(n^3+1)$ satisfy $g(n) < f(n) < g(n+1)$ for all $n \geq 2$. ▮

Propositions 4.2 and 4.4 imply that the graphs of special linear and unitary groups belonging to Case I are distinguished from each other and from the other classical groups. If we already know that G is a special linear simple group, then $\Delta(G)$ also determines the size of the underlying field, since $L(G) = (q+1)(q^3-1)$ has a unique solution for q. Once $q = p^e$ is known, $\Delta(G)$ also determines the dimension d: if k is the largest

integer such that a $\text{ppd}^{\#}(p;k)$-number divides some weight in $\Delta(G)$, then $d = k/e$. Note that $\text{ppd}^{\#}(p;k)$-numbers exist: we have $k \geq d \geq 6$, since otherwise $|V(\Delta(G))| < 7$ (cf. the tables at the end of Section 3.1), and in the case $p = 2$ we actually have $d > 7$; hence the exceptions in Zsigmondy's Theorem (cf. Section 3.1) play no role.

Similarly, if we know that G is a special unitary simple group then $\Delta(G)$ determines the size of the underlying field and the dimension of G; since we shall use this argument in Section 4.2 as well, we formulate it as a proposition.

PROPOSITION 4.5. *Suppose that G is a special unitary simple group, and $|V(\Delta(G))| \geq 7$. Then $\Delta(G)$ uniquely determines the size of the underlying field and the dimension of G.*

Proof. The size q of the underlying field is the unique solution of $L(G) = (q-1)(q^3+1)$.

Let $q = p^e$ and let d be the dimension of G. Since $|V(\Delta(G))| \geq 7$, we have $d \geq 6$ (cf. the tables at the end of Section 3.1).

Let k be the largest integer such that a $\text{ppd}^{\#}(p;k)$-number divides some weight in $\Delta(G)$. Then $j := k/2e$ is the largest odd number $\leq d$, and so $d \in \{j, j+1\}$. We have to show that $\Delta(\text{PSU}(j,q)) \ncong \Delta(\text{PSU}(j+1,q))$. If $4 \mid j+1$ then $\text{ppd}^{\#}(p;e(j+1))$-numbers exist, $\Delta(\text{PSU}(j+1,q))$ has a weight divisible by a $\text{ppd}^{\#}(p;e(j+1))$-number, and $\Delta(\text{PSU}(j,q))$ has no such weight. If $(j+1)/2$ is odd then $\text{ppd}^{\#}(p;e(j+1)/2)$-numbers exist unless $p = 2$, $e = 2$, and $j = 5$; $\Delta(\text{PSU}(j+1,q))$ has a weight divisible by a $\text{ppd}^{\#}(p;e(j+1)/2)$-number, and $\Delta(\text{PSU}(j,q))$ has no such weight. Since both $\Delta(\text{PSU}(5,4))$ and $\Delta(\text{PSU}(6,4))$ have less than seven vertices, the exceptional case when the above argument breaks down does not occur at all. ∎

The final subcase of Case I is to distinguish the symplectic and orthogonal simple groups, whenever this is possible, using our graphs.

PROPOSITION 4.6. *Let G be a symplectic or orthogonal simple group belonging to Case I. Then $\Delta(G)$ uniquely determines the size q of the underlying field of G.*

Proof. Clearly q is even if and only if all weights in $\Delta(G)$ are odd. In this case, $L_2(G) = q^2 - 1$ which determines q.

Now assume that q is odd. Then $L_3(G) = f_i(L_2(G))$ for some function f_i, $1 \leq i \leq 6$, described in (4.3). We claim that $L_2(G)$ *and* $L_3(G)$ *uniquely determine the function* f_i. For fixed $L_2(G) > 1$, we have $f_1(L_2(G)) < f_2(L_2(G)) < f_3(L_2(G))$ and $f_4(L_2(G)) < f_5(L_2(G)) < f_6(L_2(G))$, and the only possible ambiguity is when $L_2(G) = 3$ and $L_3(G) = f_3(3) = f_4(3) = 12$. The function f_3 occurs when $L_2(G) = (q^2-1)/8$ and $L_3(G) = (q^2-1)/2$, which gives $q = 5$ since $L_2(G) = 3$. The function f_4 occurs when

$L_2(G) = (q^2 - 1)/2$ and $L_3(G) = (q^4 - 1)/4$, which does not lead to an integer solution when $L_2(G) = 3$. Therefore, there is no ambiguity in this case as well.

Once we know the function f_i, q is determined uniquely. Namely, if $L_3(G) = f_1(L_2(G))$ or $L_3(G) = f_4(L_2(G))$ then $L_2(G) = (q^2 - 1)/2$; if $L_3(G) = f_2(L_2(G))$ or $L_3(G) = f_5(L_2(G))$ then $L_2(G) = (q^2 - 1)/4$; and if $L_3(G) = f_3(L_2(G))$ or $L_3(G) = f_6(L_2(G))$ then $L_2(G) = (q^2 - 1)/8$. ∎

PROPOSITION 4.7. *Let G and G^* be symplectic or orthogonal simple groups belonging to Case I. Then $\Delta(G) \ncong \Delta(G^*)$, unless G and G^* occur in cases* (i) *or* (iii) *of Theorem* 1.1.

Proof. By Proposition 4.6, $\Delta(G)$ determines the size of the underlying field of G. Suppose that G and G^* are both defined over GF(q), $q = p^e$, and $\Delta(G) \cong \Delta(G^*)$. Let k be the largest integer such that a ppd$^{\#}(p; k)$-number divides some weight in $\Delta(G)$, and define $m := k/2e$. Then $G, G^* \in \{\mathrm{PSp}(2m, q), \Omega(2m + 1, q), \mathrm{P}\Omega^+(2m + 2, q), \mathrm{P}\Omega^-(2m, q)\}$ in view of Propositions 3.18, 3.28, 3.39 and Section 3.4. Here $m \neq 2, 4$, since $|V(\Delta(G))| \geq 7$ in Case I. If $m = 3$ then $|V(\Delta(G))| \geq 7$ implies that q must be odd (the graph $\Delta(G)$ is given just before Theorem 3.25), and we are in case (iii) of Theorem 1.1 (note that $\mathrm{P}\Omega^-(6, q) \cong \mathrm{PSU}(4, q)$, so $\Delta(\mathrm{P}\Omega^-(6, q))$ has at most five vertices by Proposition 3.12 and hence does not arise here).

Suppose that $m \geq 5$. We note that $\Delta(\mathrm{PSp}(2m, q)) \cong \Delta(\Omega(2m + 1, q))$ by Section 3.4, which is case (i) of Theorem 1.1. We shall prove that there are no other ambiguities. First, we claim that $\Delta(\mathrm{P}\Omega^+(2m + 2, q))$ *is not isomorphic to* $\Delta(\mathrm{PSp}(2m, q))$ *or* $\Delta(\mathrm{P}\Omega^-(2m, q))$. Since $C(j^\varepsilon)$ is the only vertex whose weight is divisible by primitive prime power divisors of $q^j + \varepsilon 1$, an isomorphism must send the vertex $C(j^\varepsilon)$ of one graph to the vertex $C(j^\varepsilon)$ of the other graph. However, if m is odd then $C(((m - 1)/2)^+)$ and $C(((m + 3)/2)^+)$ are adjacent in $\Delta(\mathrm{P}\Omega^+(2m + 2, q))$, but they are not adjacent in $\Delta(\mathrm{PSp}(2m, q))$ or in $\Delta(\mathrm{P}\Omega^-(2m, q))$. If m is even then $C((m/2)^+)$ and $C(((m + 2)/2)^+)$ are adjacent in $\Delta(\mathrm{P}\Omega^+(2m + 2, q))$, but not in $\Delta(\mathrm{PSp}(2m, q))$ or in $\Delta(\mathrm{P}\Omega^-(2m, q))$. Similarly, $\Delta(\mathrm{PSp}(2m, q)) \ncong \Delta(\mathrm{P}\Omega^-(2m, q))$, since in the odd and even cases of m vertices $C(((m - 1)/2)^+)$ and $C(((m + 1)/2)^+)$, $C(((m - 2)/2)^+)$ and $C(((m + 2)/2)^+)$, respectively, are adjacent in $\Delta(\mathrm{PSp}(2m, q))$ but not in $\Delta(\mathrm{P}\Omega^-(2m, q))$. ∎

4.2. *Case II*

By Propositions 2.3, 3.8, 3.13 and Theorems 3.25, 3.36, 3.47, together with the explicitly described graphs appearing just before Theorem 3.12, the groups belonging to this case are those in the following table.

Group	$L_3(G)$	$L(G)$
$E_6(q)$	$\dfrac{q^2-1}{(3,q-1)}$	$\begin{cases}(q^2-1)/3 & \text{if } q \equiv 1 \pmod 6\\ q^2-1 & \text{otherwise}\end{cases}$
${}^2E_6(q)$	$\dfrac{q^2-1}{(3,q+1)}$	$\begin{cases}(q^2-1)/3 & \text{if } q \equiv 5 \pmod 6\\ q^2-1 & \text{otherwise}\end{cases}$
$E_7(q)$	$\dfrac{q^2-1}{(2,q-1)^2}$	$\dfrac{q^2-1}{(2,q-1)^2}$
$E_8(q)$	1	1
$\mathrm{PSU}(d,2)$	3 or 9	9
$\mathrm{PSU}(d,3)$	56	56
$\mathrm{P}\Omega^-(2m,3)$	4 or 20	4 or 20

The classical groups in the table can occur if d or m satisfies suitable divisibility constraints.

We will repeatedly use the graphs of the exceptional groups, as given explicitly in Section 2.

First consider the graph $\Delta(E_8(q))$. This is distinguished from the graphs of the other groups in the table as the only one with $L(G) = 1$. Moreover, there is a unique vertex of valency $|V(\Delta(E_8(q)))| - 5$. Its weight is $q^2 - 1$, so the graph determines q.

The value of $L(G)$ distinguishes the groups $\mathrm{P}\Omega^-(2m,3)$ from other groups of the list, with the exception $L(E_7(9)) = L(\mathrm{P}\Omega^-(2m,3)) = 20$. Suppose that $\Delta(E_7(9)) \cong \Delta(\mathrm{P}\Omega^-(2m,3))$ for some m. The largest k such that a $\mathrm{ppd}^{\#}(3;k)$-number occurs as a divisor of a weight in $\Delta(E_7(9))$ is $k = 36$ (namely, the prime $9^6 - 9^3 + 1 = 530713$). In $\Delta(\mathrm{P}\Omega^-(2m,3))$, the largest k such that a $\mathrm{ppd}^{\#}(3;k)$-number occurs as a divisor of a weight is $2m$, which implies $m = 18$. This is a contradiction: for m even we are in Case (ii) of Theorem 3.47, and $L(\mathrm{P}\Omega^-(2m,3)) = 4$. Therefore, the graphs $\Delta(\mathrm{P}\Omega^-(2m,3))$ differ from the graphs of other groups in the table. They also uniquely determine the value of m, since $m = k/2$ for the largest k such that a $\mathrm{ppd}^{\#}(3;k)$-number occurs as a divisor of a weight.

The value of $L(G)$ also distinguishes the groups $\mathrm{PSU}(d,3)$ and $\mathrm{PSU}(d,2)$ from the other groups, with the exception $L(E_6(13)) = L(\mathrm{PSU}(d,3)) = 56$. However, in $\Delta(E_6(13))$ there are weights divisible by 3, so $\Delta(E_6(13)) \not\cong \Delta(\mathrm{PSU}(d,3))$ for any d. Once we know that $G \cong \mathrm{PSU}(d,q)$ for some $q \in \{2,3\}$ and d, $\Delta(G)$ uniquely determines d by Proposition 4.5.

The graph $\Delta(E_7(q))$ has at least 12 vertices, which distinguishes it from $\Delta(E_6(t))$ and $\Delta({}^2E_6(t))$ for any t. Once we know that $G \cong E_7(q)$ for some q, the value $L_3(G) = (q^2-1)/(2,q-1)^2$ determines q uniquely.

Finally, suppose that $\Delta(E_6(q)) \cong \Delta({}^2E_6(t))$ for some q and t. Note that $\Delta(E_6(q))$ and $\Delta({}^2E_6(q))$ have 0 or 2 vertices of weight a power of 3. Only in $\Delta(E_6(2))$ is one of these the unique vertex with valency $|V(\Delta(G))| - 3$,

so $q \neq 2$. Taking the least common multiple of the weight of the unique vertex with valency $|V(\Delta(G))| - 3$ and the smallest weight among vertices that are powers of 3, we obtain $q^2 - 1$ in $\Delta(E_6(q))$ and $t^2 - 1$ in $\Delta({}^2E_6(t))$. Therefore, $q = t$. This is a contradiction, since $\Delta(E_6(q))$ and $\Delta({}^2E_6(q))$ have a unique isolated vertex, with weights $(q^6 + q^3 + 1)/(3, q - 1)$ and $(q^6 - q^3 + 1)/(3, q + 1)$, respectively, where $(q^6 + q^3 + 1)/(3, q - 1) \neq (q^6 - q^3 + 1)/(3, q + 1)$. In this argument, we also saw that if we know that $G \cong E_6(q)$ or ${}^2E_6(q)$ for some q, then $\Delta(G)$ uniquely determines the value of q.

4.3. *Case III*

By Propositions 3.9, 3.14, 3.24, 3.35, and 3.46, all graphs with $|V(\Delta(G))| \leq 6$ are listed explicitly in Sections 2 and 3.

Subcase 1. $|V(\Delta(G))| = 2$. All graphs in this subcase consist of two isolated vertices. In the following table, we have listed the weights $W_1 < W_2$ of these vertices.

Group	W_1	W_2
${}^2G_2(3)'$	2	7
$G_2(2)'$	3	7
PSL$(2, q)$	$(q - 1)/(2, q - 1)$	$(q + 1)/(2, q - 1)$
PSL$(3, q)$, $3 \nmid q - 1$	$q^2 - 1$	$q^2 + q + 1$
PSU$(3, q)$, $3 \nmid q + 1$	$q^2 - q + 1$	$q^2 - 1$
PSL$(4, 2)$	7	15
PSU$(4, 2)$	5	9
PSp$(4, q)$	$(q^2 - 1)/(2, q - 1)$	$(q^2 + 1)/(2, q - 1)$

It is straightforward to check that the only case in which $\Delta(G) \cong \Delta(G^*)$, where G is a member of one of the above four infinite families and $G^* \in \{{}^2G_2(3)', G_2(2)', \text{PSL}(4, 2), \text{PSU}(4, 2)\}$, is $\Delta(\text{PSL}(3, 2)) \cong \Delta(G_2(2)')$, which is case (v) of Theorem 1.1.

Concerning the four infinite families, $\Delta(\text{PSL}(2, q)) \cong \Delta(\text{PSp}(4, t))$ if and only if $q^2 = t$, which is case (ii) of Theorem 1.1. $\Delta(\text{PSL}(3, q)) \ncong \Delta(\text{PSU}(3, t))$ for any q, t, since the system of equations $q^2 - 1 = t^2 - t + 1$, $q^2 + q + 1 = t^2 - 1$ has no solution with positive prime powers q, t. Finally, $\Delta(G) \ncong \Delta(G^*)$ if $G = \text{PSL}(2, q)$ or PSp$(4, q)$ and $G^* = \text{PSL}(3, t)$ or PSU$(3, t)$: we always have $W_2(G) - W_1(G) \leq 2$, while $W_2(G^*) - W_1(G^*) \leq 2$ is possible only for $G^* \cong \text{PSU}(3, 3)$ or PSU$(3, 4)$. However, in these cases we have $W_1 = 7$, $W_2 = 8$ or $W_1 = 13$, $W_2 = 15$, and there is no $G \cong \text{PSL}(2, q)$, PSp$(4, q)$ with these parameters. Clearly the weights determine the size of the underlying field.

Subcase 2. $|V(\Delta(G))| = 3$. All graphs in this subcase consist of three isolated vertices, with weights $W_1 < W_2 < W_3$ listed below.

Group	W_1	W_2	W_3
${}^2F_4(2)'$	3	5	13
PSL(3, 4)	3	5	7
PSU(4, 3)	5	7	8
${}^2B_2(2^{2m+1})$, $m \geq 1$	$2^{2m+1} - 2^{m+1} + 1$	$2^{2m+1} - 1$	$2^{2m+1} + 2^{m+1} + 1$
$G_2(3^m)$	$3^{2m} - 3^m + 1$	$3^{2m} - 1$	$3^{2m} + 3^m + 1$

It is obvious that no two of these graphs are isomorphic, and that $\Delta(G)$ determines the size of the underlying field of G.

Subcase 3. $|V(\Delta(G))| = 4$. There are two families for which $\Delta(G)$ is a path of length 3: $\Delta(\mathrm{PSL}(4, 2^m))$ and $\Delta(\mathrm{PSU}(4, 2^m))$, for $m \geq 2$. In both families, the vertices of valency 2 have weights $2^m - 1$ and $2^m + 1$, which determines m uniquely. The two families are distinguished by the fact that a vertex of weight $2^{2m} + 1$ is adjacent to the vertex with weight $2^m - 1$ in $\Delta(\mathrm{PSU}(4, 2^m))$, and it is adjacent to the vertex with weight $2^m + 1$ in $\Delta(\mathrm{PSL}(4, 2^m))$.

In all other graphs with $|V(\Delta(G))| = 4$, the graph consists of a path of length two and of an isolated vertex. In the following table, W_i is the weight of the vertex of valency i (there are two vertices of valency 1).

Group	W_0	W_1	W_2
PSL(4, 3)	13	5, 8	4
PSL(4, 5)	31	8, 13	3
PSp(6, 2)	7	5, 9	3
$P\Omega^+(8, 2)$	7	5, 9	3
PSL(6, 2)	31	5, 63	3
PSL(3, q), $3 \mid q - 1$, $q > 4$	$(q^2 + q + 1)/3$	$(q - 1)_3, (q - 1)_2(q + 1)$	$(q - 1)/3$
PSU(3, q), $3 \mid q + 1$, $q > 2$	$(q^2 - q + 1)/3$	$(q + 1)_3, (q + 1)_2(q - 1)$	$(q + 1)/3$
${}^3D_4(q)$	$q^4 - q^2 + 1$	$(q + 1)_3(q^2 - q + 1)$, $(q - 1)_3(q^2 + q + 1)$	$q^2 - 1$
$G_2(q)$, $3 \mid q - 1$	$q^2 - q + 1$	$(q^2 + q + 1)/3$, $(q^2 - 1)(9, q^2 - 1)/9$	3
$G_2(q)$, $3 \mid q + 1$, $q > 2$	$q^2 + q + 1$	$(q^2 - q + 1)/3$, $(q^2 - 1)(9, q^2 - 1)/9$	3
PSL(5, q)	$\dfrac{q^5 - 1}{(q - 1)(5, q - 1)}$	$(q^2 - 1)_2(q^2 + 1)$, $(q - 1)_3(q - 1)_5(q^2 + q + 1)$	$\dfrac{q^2 - 1}{(5, q - 1)}$
PSU(5, q)	$\dfrac{q^5 + 1}{(q + 1)(5, q + 1)}$	$(q^2 - 1)_2(q^2 + 1)$, $(q + 1)_3(q + 1)_5(q^2 - q + 1)$	$\dfrac{q^2 - 1}{(5, q + 1)}$

PROPOSITION 4.8. *If G and G^* are nonisomorphic groups on the above list such that $W_2(G) = W_2(G^*) = 3$ and $\Delta(G) \cong \Delta(G^*)$, then $\{G, G^*\} = \{\mathrm{PSp}(6,2), \mathrm{P}\Omega^+(8,2)\}$.*

Proof. First we prove that if $G = G_2(q)$ and $G^* = G_2(t)$, then $q = t$. If $3 \mid q-1$ and $3 \mid t-1$ then $W_0 = q^2 - q + 1 = t^2 - t + 1$ and so $q = t$. Similarly, if $3 \mid q+1$ and $3 \mid t+1$ then $W_0 = q^2 + q + 1 = t^2 + t + 1$ and $q = t$. Finally, it is impossible that $3 \mid q-1$ and $3 \mid t+1$, since $W_0 = q^2 - q + 1 = t^2 + t + 1$ implies that $q = t+1$, which contradicts the mod 3 divisibility constraints on q and t.

Besides the groups $G_2(q)$, there are nine groups with $W_2 = 3$: in addition to those where the listed value of W_2 is 3, they are $\mathrm{PSU}(3,8)$, ${}^3D_4(2)$, $\mathrm{PSL}(5,2)$, $\mathrm{PSU}(5,2)$, and $\mathrm{PSU}(5,4)$. Listing these nine sets of weights explicitly, we see that all groups not isomorphic to $G_2(q)$ and with $W_2 = 3$ satisfy $W_0 \le 41$, and with the exception of $\{G, G^*\} = \{\mathrm{PSp}(6,2), \mathrm{P}\Omega^+(8,2)\}$, the set of weights distinguishes them. This exceptional case is included in case (iii) of Theorem 1.1. Also, these nine graphs are not isomorphic to $\Delta(G_2(q))$ for any q, since $W_0 \le 41$ is possible only for $G_2(4)$ and $G_2(5)$, but these two cases provide different sets of weights than the previous nine. ∎

We now turn to the groups with $W_2 \ge 4$. It is straightforward to check that $\Delta(\mathrm{PSL}(4,3))$ is distinguished from the others. The graphs $\Delta(\mathrm{PSL}(3,q))$ and $\Delta(\mathrm{PSU}(3,q))$ are distinguished as the only ones where one of the weights W_1 is a power of 3 (note that there are such weights in $\Delta({}^3D_4(2))$ and $\Delta(\mathrm{PSU}(5,2))$, but in these graphs $W_2 = 3$). We have $\Delta(\mathrm{PSL}(3,q)) \not\cong \Delta(\mathrm{PSU}(3,t))$ for any q, t, since comparing the values of W_0 and W_2, we get the system of equations $(q^2+q+1)/3 = (t^2-t+1)/3$, $(q-1)/3 = (t+1)/3$ having no solution with $t > 0$. Once we know that $G \cong \mathrm{PSL}(3,q)$ for some q, W_2 determines q, and the same remark holds for the groups $\mathrm{PSU}(3,q)$.

Comparing W_0 and W_2 also distinguishes $\Delta({}^3D_4(q))$ from $\Delta(\mathrm{PSL}(5,t))$. Namely, if $W_2 = q^2 - 1 = t^2 - 1$ then $q = t$, and $q^4 - q^2 + 1 < (t^5 - 1)/(t-1)$. If $W_2 = q^2 - 1 = (t^2-1)/5$ then eliminating q^2 from the equation $W_0 = q^4 - q^2 + 1 = (t^5-1)/5(t-1)$ leads to a fourth-order equation for t, with $t = 1$ as the only integer solution.

The graphs $\Delta({}^3D_4(q))$ and $\Delta(\mathrm{PSU}(5,t))$ can be distinguished by the same argument. Once we know that $G \cong {}^3D_4(q)$ for some q, the value of W_2 determines q uniquely.

Finally, we distinguish the graphs $\Delta(\mathrm{PSL}(5,q))$ and $\Delta(\mathrm{PSU}(5,t))$ by considering the least common multiple M of the weights W_2 and W_1. We have $M(\mathrm{PSL}(5,q)) = (q^4-1)(q^2+q+1)$ and $M(\mathrm{PSU}(5,t)) = (t^4-1)(t^2-t+1)$, and these two values cannot be equal: for the functions $f(n) = (n^4-1)(n^2+n+1)$ and $g(n) = (n^4-1)(n^2-n+1)$, we have

$g(n) < f(n) < g(n+1)$ for all integers $n \geq 2$. Once we know that $G \cong \mathrm{PSL}(5, q)$ for some q, the value of M determines q, and the same remark holds for the groups $\mathrm{PSU}(5, q)$.

Subcase 4. $|V(\Delta(G))| = 5$. Not considering the weights, graphs in this subcase fall into three isomorphism classes, reflected by the grouping in the following table.

	Group
(A)	${}^2G_2(3^{2m+1})$, $m \geq 1$
	$\mathrm{PSU}(6, 2)$
(B)	$\mathrm{PSL}(4, q)$, $q \geq 7$ odd
	$\mathrm{PSU}(4, q)$, $q \geq 5$ odd
	$\mathrm{PSp}(6, 2^m)$, $m \geq 2$
	$\mathrm{P}\Omega^+(8, 2^m)$, $m \geq 2$
(C)	$\mathrm{PSp}(8, q)$
	$\mathrm{P}\Omega^-(8, q)$
	$\Omega(9, q)$
	$\mathrm{P}\Omega^+(10, 2)$
	$\mathrm{P}\Omega^-(10, 2)$

In Class (A), there is a unique vertex of valency 2, with weight 2 in $\Delta({}^2G_2(3^{2m+1}))$ and 3 in $\Delta(\mathrm{PSU}(6, 2))$. The graph $\Delta({}^2G_2(3^{2m+1}))$ also determines the value of m, since the largest weight is $3^{2m+1} + 3^{m+1} + 1$.

In Class (B), $\Delta(\mathrm{PSp}(6, 2^m)) \cong \Delta(\mathrm{P}\Omega^+(8, 2^m))$, which is a special case of Theorem 1.1(iii). These graphs are distinguished from $\Delta(\mathrm{PSL}(4, q))$ and $\Delta(\mathrm{PSU}(4, q))$ by the fact that all weights are odd. The unique vertex of valency two has weight $2^{2^m} + 1$, which determines m uniquely.

In $\Delta(\mathrm{PSL}(4, q))$ and $\Delta(\mathrm{PSU}(4, q))$, the least common multiple of the weights of the vertices of valency at least two is $q^2 - 1$, which determines q. For fixed q, $\Delta(\mathrm{PSL}(4, q))$ and $\Delta(\mathrm{PSU}(4, q))$ are distinguished by the fact that the least common multiple of all weights is $(q^4 - 1)(q^3 - 1)/2(q - 1)$ and $(q^4 - 1)(q^3 + 1)/2(q + 1)$, respectively.

In Class (C), $\Delta(\mathrm{PSp}(8, q)) \cong \Delta(\mathrm{P}\Omega^-(8, q)) \cong \Delta(\Omega(9, q))$, which is case (iv) of Theorem 1.1. There is a unique isolated vertex; its weight is $(q^4 + 1)/(2, q - 1)$, which uniquely determines q (note that whether q is odd or even is determined by whether or not there are even weights in the graph). In $\Delta(\mathrm{P}\Omega^+(10, 2))$ and $\Delta(\mathrm{P}\Omega^-(10, 2))$ the unique isolated vertex has weight 31 and 17, respectively, which distinguishes them from each other and from $\Delta(\mathrm{PSp}(8, q))$, with the possible exception of $\Delta(\mathrm{PSp}(8, 2))$. However, $\Delta(\mathrm{PSp}(8, 2))$ and $\Delta(\mathrm{P}\Omega^-(10, 2))$ are distinguished by the weights of vertices of valency one.

Subcase 5. $|V(\Delta(G))| = 6$. Not considering the weights, graphs in this subcase fall into seven isomorphism classes, reflected by the grouping in the following table.

	Group
(A)	$F_4(2^m)$
(B)	${}^2F_4(2^{2m+1})$, $m \geq 1$
(C)	PSL(6, 3)
(D)	PSU(6, 3)
(E)	PSL(6, 2^{2m+1}), $m \geq 1$
	PSU(6, 2^{2m})
(F)	PSp(6, 3)
	$\Omega(7, 3)$
	$P\Omega^+(8, 3)$
	$P\Omega^+(12, 2)$
	PSL(7, q), $7 \nmid q - 1$
	PSU(7, q), $7 \nmid q + 1$
(G)	$P\Omega^+(10, 2^m)$, $m \geq 2$
	$P\Omega^-(10, 2^m)$, $m \geq 2$

In Class (A), there is a unique vertex of valency 3; its weight is $2^{2m} - 1$, which determines m. In Class (B), there is a unique vertex of valency 2; its weight is $2^{2m+1} - 1$, which again determines m. In Class (E), there are two vertices of valency 4, and in both families their weights are $q - 1$ and $q + 1$. This determines q uniquely, and the parity of $\log_2 q$ indicates whether we have $\Delta(\mathrm{PSL}(6, q))$ or $\Delta(\mathrm{PSU}(6, q))$.

In Class (F), $\Delta(\mathrm{PSp}(6, 3)) \cong \Delta(\Omega(7, 3)) \cong \Delta(P\Omega^+(8, 3))$, which is a special case of Theorem 1.1(iii). In this class, $\Delta(G)$ has a unique vertex of valency 4. Denoting its weight by W_4, we have $W_4(\mathrm{PSp}(6, 3)) = 2$, $W_4(P\Omega^+(12, 2)) = 3$, and $W_4(\mathrm{PSL}(7, q)) = W_4(\mathrm{PSU}(7, q)) = q^2 - 1$. Hence W_4 determines the value of q uniquely and distinguishes $\Delta(\mathrm{PSL}(7, q))$, $\Delta(\mathrm{PSU}(7, q))$, and $P\Omega^+(12, 2)$ from $\Delta(\mathrm{PSp}(6, 3))$. If $W_4 = 3$ (and so $q = 2$) then the unique isolated vertex has weight 127, 43, and 31 in $\Delta(\mathrm{PSL}(7, 2))$, $\Delta(\mathrm{PSU}(7, 2))$, and $\Delta(P\Omega^+(12, 2))$, respectively. For fixed $q > 2$, $\Delta(\mathrm{PSL}(7, q))$ and $\Delta(\mathrm{PSU}(7, q))$ are distinguished by the fact that the unique isolated vertex has weight $(q^7 - 1)/(q - 1)$ and $(q^7 + 1)/(q + 1)$ respectively.

In Class (G), there are two vertices of valency 4, with weights $2^m - 1$ and $2^m + 1$. This determines the value of m. Finally, $\Delta(P\Omega^+(10, 2^m)) \ncong \Delta(P\Omega^-(10, 2^m))$ because a $\mathrm{ppd}^{\#}(2; 10m)$-number divides some weight in $\Delta(P\Omega^-(10, 2^m))$, while there is no such weight in $\Delta(P\Omega^+(10, 2^m))$.

This completes the proof of Theorem 1.1.

5. ALGORITHMIC CONSEQUENCE: THEOREM 1.2

5.1. *Background*

Currently, the most active area of Computational Group Theory is the design and implementation of matrix group algorithms. There are two

basic approaches. One of them is the so-called matrix group project: it tries to determine which class of Aschbacher's classification [Asch1] of subgroups of $\mathrm{GL}(d, q)$ contains a given matrix group G [NiP1, NiP2, CLG1, HR, HLOR1, HLOR2, LGO]. In almost all cases of Aschbacher's classification, there is a normal subgroup N naturally associated with the geometry of G; the goal is to construct generators for N and recursively handle N and G/N. This approach bottoms out when a quasisimple group acting absolutely irreducibly is reached.

The other approach [BB] considers matrix groups as *black-box groups*. The elements of a black-box group G are encoded as 0−1 strings of uniform length n. An element may be encoded in different ways, and not every string has to represent a group element. The group operations are performed by an oracle (the "black box"). Given strings representing $g, h \in G$, the oracle can compute strings representing gh and g^{-1} and decide whether or not $g = h$. Note that $|G| \leq 2^n$: we have an upper bound on $|G|$. It is possible that the oracle can perform the group operations in an overgroup $\overline{G}$ of G; in this case, the oracle can decide whether a string represents an element of $\overline{G}$ (and so group operations are defined), but we do not assume that the oracle can recognize whether an element of $\overline{G}$ is in G. For example, if $G \leq \mathrm{GL}(d, q)$ is a matrix group then $\overline{G} = \mathrm{GL}(d, q)$ is such a natural overgroup.

Algorithms for permutation groups or matrix groups usually try to exploit the specific features of the representation of the group they work with. By contrast, a black-box group algorithm does not rely on such specific features of the group representation or even on particulars of how the group operations are performed. Because of the generality of the definition, algorithms for black-box groups may have limitations, and we may need additional oracles. In Theorem 1.2, we shall consider black-box groups with an oracle computing orders of group elements.

The Babai−Beals method [BB] constructs generators for the simple normal subgroups in the socle of $G/O_\infty(G)$, where $O_\infty(G)$ is the largest solvable normal subgroup of the input group G. Therefore, further progress here also depends on the availability of constructive recognition algorithms for simple groups, and there is a rapidly growing list [Bra, Bro, Bro2, BK, Ce, CLG2, CFL, KS1, KM, BP, BLNPS] of such algorithms. We formalize constructive recognition of simple groups the following way (cf. [KS2]).

DEFINITION 5.1. Let $\mathscr{F}$ be a family of simple groups and let $f: \mathscr{F} \to \mathbb{R}$ be a function taking positive values. We say that $\mathscr{F}$ is *black-box f-recognizable* if, whenever a group $G = \langle \mathscr{S} \rangle$ isomorphic to a member of $\mathscr{F}$ is given as a black-box group encoded by strings of length n and, in the case of

Lie-type G, *the characteristic of G is given*, there are Las Vegas algorithms for the following:

(i) Find the isomorphism type of G.

(ii) Find a new set $\mathscr{S}^*$ of size $O(n)$ generating G, and a presentation of length $O(n^2)$ in terms of $\mathscr{S}^*$. (This presentation proves that G has the isomorphism type determined in (i).)

(iii) Given $g \in G$, find a straight-line program of length $O(n)$ from $\mathscr{S}^*$ to g.

Moreover,

(iv) The algorithms for (i)–(iii) run in time $O((\xi + \mu)f(G)n^c)$, where ξ is an upper bound on the time requirement per element for the construction of independent, (nearly) uniformly distributed random elements of G, μ is an upper bound on the time required for each group operation in G, and c is an absolute constant.

A *straight-line program of length m* reaching some $g \in G$ can be thought of as a sequence of group elements $(g_1, \ldots, g_m)$ such that $g_m = g$ and for each i one of the following holds: $g_i \in \mathscr{S}^*$, or $g_i = g_j^{-1}$ for some $j < i$, or $g_i = g_j g_k$ for some $j, k < i$. More precisely, since we do not want to store the group elements themselves, a straight-line program reaching g is a sequence of expressions $(w_1, \ldots, w_m)$ such that, for each i, either w_i is a symbol for some element of $\mathscr{S}^*$, or $w_i = (w_j, -1)$ for some $j < i$, or $w_i = (w_j, w_k)$ for some $j, k < i$, such that if the expressions are evaluated in the obvious way then the value of w_m is g. This more abstract definition not only requires less memory, but also *enables us to construct a straight-line program in one representation of G and evaluate it in another*, which is an important feature of many matrix group algorithms.

Recall that a randomized algorithm is called *Monte Carlo* if for every $\varepsilon > 0$, it can be achieved that the probability of incorrect output is less than ε. An important subclass of Monte Carlo algorithms is the class of *Las Vegas* algorithms, which can recognize that the output is incorrect. In other words, the output of a Las Vegas algorithm is always correct, but the algorithm may report failure with a small probability.

We say that an algorithm outputs an *ε-uniformly distributed element x* in a group G if $(1 - \varepsilon)/|G| < \text{Prob}(x = g) < (1 + \varepsilon)/|G|$ for all $g \in G$. *Nearly uniform* means ε-uniform for some $\varepsilon \leq 1/2$.

By a theorem of Babai [Ba], nearly uniform random elements in black-box groups can be constructed using polynomially many group operations.

THEOREM 5.2 [Ba]. *Let c and C be given positive constants. Then there is a Monte Carlo algorithm which, when given a black-box group G of order at most M and any set of generators $\mathscr{S}$ of G, sets up a data structure for the*

construction of ε-uniformly distributed elements for $\varepsilon = M^{-c}$, at a cost of $O(\log^5 M + |\mathscr{S}|\log\log M)$ group operations. The probability that the algorithm fails is at most M^{-C}.

If the algorithm succeeds, it permits the construction of ε-uniformly distributed, independent random elements of G at a cost of $O(\log M)$ group operations per element.

Using the terminology of Definition 5.1, the main result of [KS1, KM] can be stated as follows:

THEOREM 5.3 [KS1, KM]. *Let*

$$f(G) = \begin{cases} q^3 & \text{if } G \cong \mathrm{PSU}(d,q) \text{ for some } d \\ q & \text{for all other classical simple } G \text{ defined on a vector space} \\ & \quad \text{over } \mathrm{GF}(q) \\ q^{52} & \text{for } {}^2F_4(q) \\ q^3 & \text{for all other exceptional simple } G \text{ defined over } \mathrm{GF}(q). \end{cases}$$

Then Lie-type simple groups, with the possible exception of the groups ${}^2G_2(q)$, comprise a black-box f-recognizable family.

We note that in [KS1, KM] a new generating set $\mathscr{S}^*$ satisfying Definition 5.1(iii) was found within the required time bound in the groups $G \cong {}^2G_2(q)$ as well, but it is an open problem whether these groups have presentations of length $O(\log^2 |G|)$. For the other Lie-type simple groups G, such short presentations were constructed in [BGKLP; HS; Suz, p. 128]. The timing for the groups ${}^2F_4(q)$ undoubtedly can be greatly decreased; the timing given reflects a brute force method and is not contained in any of the above references. (The exponent 52 can be reduced quite a bit just by constructing and then using the Bruhat decomposition in this group.)

Actually, in [KS1] we prove more than Theorem 5.3 for the classical groups: an isomorphism λ with a (projective) group of matrices in the correct dimension is constructed, defined by the images of generators, together with procedures to compute the image of any element of G under λ or of any element of $G\lambda$ under λ^{-1}. These procedures are very useful for further computations with G.

In this paper, we use the constructive recognition algorithm of Theorem 5.3 as a Monte Carlo algorithm, to decide whether the input group is defined over some *small* field $\mathrm{GF}(q)$ (we shall define "small" precisely in Section 5.3). We *assume* that the input group is simple and has a certain isomorphism type; if our assumption is correct then, with high probability, the algorithm proceeds as in Definition 5.1 to provide a proof of the assumption. If the algorithm reports failure then we do not know which of

the following two possibilities occurred: either the assumption was correct but the algorithm did not succeed because it used an unlucky sequence of random bits, or the input group did not have the assumed isomorphism type. However, we know that with high probability the latter case occurred.

The present paper grew out of the need to determine the characteristic of a given simple black-box group of Lie type, which is needed as part of the input in the recognition algorithm of Theorem 5.3.

5.2. *Probability Estimates*

The idea behind the algorithm constructing $\Delta(G)$ is not difficult: we compute the orders of some random elements of G. The sample should be large enough so that, for each pair of prime powers $\{r^a, s^b\}$, $r, s \neq p$, for which there exists an element of order $\mathrm{lcm}(r^a, s^b)$ in G, there is an element of the sample with order divisible by $\mathrm{lcm}(r^a, s^b)$. On the other hand, the sample should be small enough that it contains no elements of order divisible by p. As we shall see, these two requirements are contradictory when G is defined over $\mathrm{GF}(q)$ for small enough q, which causes some complications. In this section we give the necessary estimates for the number of random elements to be taken which ensures that all required orders appear (or do not appear, respectively) in the sample.

The frequency of elements of order divisible by p was estimated by Guralnick and Lübeck [GL]:

THEOREM 5.4 [GL]. *Let G be a simple group of Lie type of characteristic p, defined over $\mathrm{GF}(q)$. Then the proportion of elements in G of order divisible by p is less than $3/(q-1) + 2/(q-1)^2$.*

In exceptional groups, we use a lower bound by Lübeck [Lü] for the proportion of elements of order divisible by $\mathrm{lcm}(r^a, s^b)$:

THEOREM 5.5 [Lü, Corollary 2.2(b)]. *Let G be of rank at most 8 and defined over $\mathrm{GF}(q)$ with $q = p^e > 63848$. Assume that G contains an element of order m, for some number m not divisible by p which has at most three different prime divisors. Then the proportion of regular semisimple elements of G which have order divisible by m is at least $1/(1.8 \cdot 10^{13})$.*

We handle the classical groups using the following theorem:

THEOREM 5.6. *Let S be any of the simple classical groups defined on a vector space of dimension d over $\mathrm{GF}(p^e)$.*

(1) *If r^a is a vertex of $\Gamma(S)$, then there are at least $|S|/6d^2$ elements of S of order divisible by r^a.*

(2) *If r^a, s^b are adjacent vertices of $\Gamma(S)$, then there are at least $|S|/6d^3$ elements of S of order divisible by $\mathrm{lcm}(r^a, s^b)$.*

(3) *Assume that r^a and s^b are adjacent vertices of $\Delta(S)$ such that, for some positive integers I, J, $r^a \mid p^{eI} - 1$ but $r^a \nmid p^k - 1$ for $1 \le k < eI$ and $s^b \mid p^{eJ} - 1$ but $s^b \nmid p^k - 1$ for $1 \le k < eJ$. If $I + J \ge d - 1$ then there are at least $|S|/12d^2$ elements of S of order divisible by* $\mathrm{lcm}(r^a, s^b)$.

Proof. The method of proof is a straightforward modification of standard ideas [Bra, Bro, BK, CFL, KM, KS1, NiP2]. We focus on (2) (with $r \ne s$) and temporarily ignore the easier case $\mathrm{PSL}(d, q)$ until after dealing with the other cases. First note that we can lift the desired result to the linear group, so we now assume that $S = \mathrm{Sp}(V)$, $\Omega(V)$, or $\mathrm{SU}(V)$. Let G denote the group of *all* isometries of V.

We will use cyclic subgroups (tori) $A < G$ satisfying one of the following conditions, where $V_A = [V, A]$ is nonsingular and $d_A = \dim V_A$:

(i) A is irreducible on V_A and has order $q^{d_A/2} + 1$ or

(ii) A has two totally singular irreducible constituents of dimension $d_A/2$ on V_A and has order $q^{d_A/2} - 1$.

In each case the torus A satisfies $C_G(A) = A \times C_G(V_A)$ and $|N_G(A)/C_G(A)| \le d_A$.

The constructions in Propositions 3.3, 3.19, 3.29, and 3.40, as well as the versions of them implicitly contained in Sections 3.2 and 3.4, show that an element of the desired order occurs in $(AB) \cap S \bmod Z(S)$, where A and B are tori of the above sorts such that the following hold:

$r^a \mid |A|$ and $s^b \mid |B|$;

if $r^a s^b \nmid |A|$ then V_A and V_B are nonisometric and perpendicular; and

if $r^a s^b \mid |A|$ then either

$A = B$,

S is unitary, $d_B = 1$, and V_A and V_B are perpendicular (this possibility is needed in order to deal with the determinant condition when r or s divides $q + 1$), or

S is orthogonal, $d_B = 2$, and V_A and V_B are perpendicular (this possibility is needed in order to deal with the spinor norm condition when r or s is 2).

Let C be a torus behaving as in (i) or (ii) such that $V_C = (V_A + V_B)^\perp$ (use $C = 1$ and $d_C = 1$ if either $V = V_A + V_B$ or $V_A + V_B$ is a hyperplane of the orthogonal space V). Write $X = ABC$. We will estimate the number of elements of order divisible by $r^a s^b$ contained in $X \cap S \bmod Z(S)$.

Since V_A, V_B, and V_C are the only possible irreducible constituents of $X \cap S$, we have $C_S(X) = C_S(X \cap S) = X \cap S$. For the same reason, in general $|N_S(X)/C_S(X)| \le 2d_A d_B d_C$: it is possible that V_C is isometric to V_A or V_B; recall that V_A and V_B are either equal or not isometric unless V

is either unitary and $d_A = d_B = 1$, or orthogonal and $d_A = d_B = 2$, in which cases we have the additional possibility that $d_A = d_B = d_C = 1$ or 2, $d = 3d_A$ and $|N_S(X)/C_S(X)| = 3!d_A d_B d_C$. Excluding the latter case, the number of elements of the desired order is at least $|S : N_S(X)|\,|X \cap S|(1 - 1/r)(1 - 1/s) \geq |S|(1/2)(2/3)/2d_A d_B d_C \geq |S|/6d^3$. In the excluded cases we obtain at least $|S|(1/2)(2/3)/6d_A d_B d_C > |S|/6d^3$ elements.

The case $\mathrm{PSL}(d, q)$ is handled as above, using tori A that are irreducible on $[V, A]$. We consider decompositions $V = V_A \oplus V_B$ and $V = V_A \oplus V_B \oplus V_C$, where $d_B = 1$ in the latter case, and obtain the same estimates as before.

In part (1) we also consider a decomposition of one of the following types: $V = V_A \perp V_B$ or $V = V_A \oplus V_B$, or else $V = V_A \perp V_B \perp V_C$ or $V = V_A \oplus V_B \oplus V_C$ with $d_B \leq 2$, and proceed as before.

Finally, consider (3) (note that I and J are in general not the same as the integers i, j employed in Section 3). If we can choose $A = B$ or $d_B \leq 2$ then let C be as before (as noted above, we single out the cases $d_B = 1$ and $d_B = 2$ in order to deal with determinants and spinor norms). Otherwise $d_A \geq I$ and $d_B \geq J$, and hence, with V_C as before, $d_C \leq d - I - J \leq 1$. In either case we find that the number of desired elements is at least $|S|(1/2)(2/3)/2(d_A 2d_C) \geq |S|/12d^2$ or $|S|(1/2)(2/3)/2d_A d_B \geq |S|/6d^2$, or else $|S|(1/2)(2/3)/6d_A d_B d_C > |S|/12d^2$ when $d = 3$, $d_A = d_B = d_C = 1$. ∎

5.3. *The Algorithm for Theorem* 1.2

Let $N = \max\{\lceil 5.4 \cdot 10^{13} \log n \rceil, \lceil 144 n^{3/2} \log n \rceil\}$. First, we handle the possibility that the input group G is defined over $\mathrm{GF}(q)$ for some $q \leq 1 + 5Nn$. To this end, for each prime power $q = p^e \leq 1 + 5Nn$, we *assume* that G is defined over $\mathrm{GF}(q)$ and run the constructive recognition algorithm of Theorem 5.3. If our assumption is correct then with high probability this algorithm finds the isomorphism type of G and checks that G satisfies a presentation for that particular isomorphism type, thereby *proving* that the assumption is correct. The running time in Theorem 5.3 is polynomial in n and q, and hence it is polynomial in the input length since q is bounded by a polynomial function of n.

If for all $q \leq 1 + 5Nn$ the constructive recognition algorithm fails then with high probability, G is defined over a field of size greater than $1 + 5Nn$. Let p denote the sought-after characteristic of G. Take N random elements of G, and collect their orders in a list L. By Theorem 5.4, with probability at least $(1 - 5/(q-1))^N > 1 - 5N/(q-1) \geq 1 - 1/n$, there is no element order in L divisible by p. On the other hand, we claim that *with probability at least* $1 - 1/n$, *for each pair of prime powers* $\{r^a, s^b\}$ such that G contains an element of order $\mathrm{lcm}(r^a, s^b)$ *and* $r, s \neq p$,

there is an order on the list L that is divisible by $\operatorname{lcm}(r^a, s^b)$. There are at most $\log |G| \leq n$ prime powers that are element orders in G, so there are at most n^2 pairs $\{r^a, s^b\}$ such that G contains an element of order $\operatorname{lcm}(r^a, s^b)$. For any such pair $\{r^a, s^b\}$, if G is exceptional then the probability that a random element of G has order divisible by $\operatorname{lcm}(r^a, s^b)$ is at least $1/1.8 \cdot 10^{13} \geq 3 \log n/N$ by Theorem 5.5. On the other hand, if G is classical defined on a vector space of dimension d then the probability that a random element of G has order divisible by $\operatorname{lcm}(r^a, s^b)$ is at least $1/6d^3 > 1/48 \log^{3/2} |G| \geq 1/48n^{3/2} \geq 3 \log n/N$ by Theorem 5.6. Hence, in both cases the probability that none of N random elements has order divisible by $\operatorname{lcm}(r^a, s^b)$ is less than $(1 - 3 \log n/N)^N < 1/n^3$, and so the probability that there exists a pair $\{r^a, s^b\}$ for which none of N random elements has order divisible by $\operatorname{lcm}(r^a, s^b)$ is less than $n^2/n^3 = 1/n$, proving our claim.

Suppose that L contains no order divisible by p and that, for all pairs of prime powers $\{r^a, s^b\}$ such that G contains an element of order $\operatorname{lcm}(r^a, s^b)$ and $r, s \neq p$, there is an order on the list L which is divisible by $\operatorname{lcm}(r^a, s^b)$. What remains to show is that *the graph $\Delta(G)$ can be constructed from L in time polynomial in n*. The order of any element of G is obviously at most $|G| \leq 2^n$, so L consists of numbers of length at most n digits. Hence the four basic arithmetic operations and taking greatest common divisors can be performed in polynomial time with the elements of L [Kn, p. 343, Corollary L].

Our first goal is to compute pairwise relatively prime numbers $P_1, \ldots, P_m$ such that any element order $|g|$ on the list L can be written in the form $|g| = \prod_{i=1}^m P_i^{\alpha_i}$ for some nonnegative integers α_i. Such a set $\mathscr{P} = \{P_1, \ldots, P_m\}$ can be constructed by the following folklore algorithm (cf. [BB, p. 56]). Initialize $\mathscr{P}$ as the set of element orders in L. While there are $a, b \in \mathscr{P}$ which are not relatively prime, delete a and b from $\mathscr{P}$ and add $\gcd(a, g)$, $a/\gcd(a, b)$, and $b/\gcd(a, b)$ to $\mathscr{P}$. The procedure runs in polynomial time since at each modification of $\mathscr{P}$, the product of elements of $\mathscr{P}$ decreases at least by a factor of 2. For an efficient version of this algorithm, see [BDS].

After the numbers $P_1, \ldots, P_m$ are computed, we construct a graph $\Sigma(G)$ the following way. The vertices of $\Sigma(G)$ are the numbers P_i^α which occur as divisors of some element order in L, and two numbers P_i^α, P_j^β are connected if and only if they divide the same element of L. Finally, we compute the weighted quotient graph $\Psi(G)$ of $\Sigma(G)$, defined by the rule that two vertices are equivalent if they have the same neighbors, and the weight of an equivalence class is the least common multiple of the vertices in the equivalence class. The following observation finishes the construction of $\Delta(G)$:

PROPOSITION 5.7. *The graphs $\Delta(G)$ and $\Psi(G)$ are isomorphic.*

Proof. For each vertex r^a of $\Gamma(G)$, there is an element of L divisible by r^a, so there is a unique index $i(r)$ and a unique exponent $\alpha(a,r)$ such that $r^a \mid P_{i(r)}^{\alpha(a,r)}$ but $r^a \nmid P_{i(r)}^{\alpha(a,r)-1}$. The crucial observation is that, if some $|g| \in L$ is divisible by r^a then $|g|$ is divisible by $P_{i(r)}^{\alpha(a,r)}$ as well: when $|g|$ is written as a product of powers of the numbers P_j, one of the terms is divisible by r^a and hence must be $P_{i(r)}^{\alpha}$ with $\alpha \geq \alpha(a,r)$, by the definition of this number.

We claim that $(*)$ *vertices* $r_1^{a_1}, r_2^{a_2}$ *of* $\Gamma(G)$ *are connected if and only if* $P_{i(r_1)}^{\alpha(a_1,r_1)}$ *and* $P_{i(r_2)}^{\alpha(a_2,r_2)}$ *are connected in* $\Sigma(G)$. For, if $r_1^{a_1}$ and $r_2^{a_2}$ are connected then there is an element of L divisible by $\operatorname{lcm}(r_1^{a_1}, r_2^{a_2})$; by the remark in the previous paragraph, such an element of L is divisible by $\operatorname{lcm}(P_{i(r_1)}^{\alpha(a_1,r_1)}, P_{i(r_2)}^{\alpha(a_2,r_2)})$. Conversely, if L has an element of order divisible by $\operatorname{lcm}(P_{i(r_1)}^{\alpha(a_1,r_1)}, P_{i(r_2)}^{\alpha(a_2,r_2)})$ then G has an element of order $r_1^{a_1} r_2^{a_2}$. This proves $(*)$.

Now define a map $\lambda: V(\Delta(G)) \to V(\Psi(G))$ as follows: for $v \in V(\Delta(G))$ take any $r^a \in V(\Gamma(G))$ with $r^a \in v$, and let $\lambda(v)$ be the equivalence class of $P_{i(r)}^{\alpha(a,r)}$ in $\Sigma(G)$. Note that λ is well-defined: if $r_1^{a_1}, r_2^{a_2} \in v$ then we need to show that $P_{i(r_1)}^{\alpha(a_1,r_1)}$ and $P_{i(r_2)}^{\alpha(a_2,r_2)}$ are equivalent in $\Sigma(G)$. Let $P^\alpha \in V(\Sigma(G))$ be connected to $P_{i(r_1)}^{\alpha(a_1,r_1)}$, and consider $r_3^{a_3} \in V(\Gamma(G))$ with $P_{i(r_3)}^{\alpha(a_3,r_3)} = P^\alpha$. By $(*)$, $r_1^{a_1}$ and $r_3^{a_3}$ are connected in $\Gamma(G)$. Since $r_1^{a_1}$ and $r_2^{a_2}$ are equivalent, $r_2^{a_2}$ and $r_3^{a_3}$ are connected. Applying $(*)$ in the other direction we see that $P_{i(r_3)}^{\alpha(a_3,r_3)} = P^\alpha$ and $P_{i(r_2)}^{\alpha(a_2,r_2)}$ are connected. Interchanging the roles of $r_1^{a_1}$ and $r_2^{a_2}$, it follows that $P^\alpha \in V(\Sigma(G))$ is connected to $P_{i(r_1)}^{\alpha(a_1,r_1)}$ if and only if it is connected to $P_{i(r_2)}^{\alpha(a_2,r_2)}$, as required.

Next we show that $v_1, v_2 \in V(\Delta(G))$ are connected if and only if $\lambda(v_1), \lambda(v_2) \in \Psi(G)$ are connected. Namely, consider $r_1^{a_1} \in v_1$ and $r_2^{a_2} \in v_2$. By the definition of the quotient graph $\Delta(G)$, v_1 and v_2 are connected if and only if $r_1^{a_1}$ and $r_2^{a_2}$ are connected in $\Gamma(G)$. By $(*)$, $r_1^{a_1}$ and $r_2^{a_2}$ are connected if and only if $P_{i(r_1)}^{\alpha(a_1,r_1)}$ and $P_{i(r_2)}^{\alpha(a_2,r_2)}$ are connected in $\Sigma(G)$. By the definition of the quotient graph $\Psi(G)$, $P_{i(r_1)}^{\alpha(a_1,r_1)}$ and $P_{i(r_2)}^{\alpha(a_2,r_2)}$ are connected if and only if $\lambda(v_1)$ and $\lambda(v_2)$ are connected.

The map λ is injective. For, if v_1 and v_2 are two different vertices of $\Delta(G)$ then, for $r_1^{a_1} \in v_1$ and $r_2^{a_2} \in v_2$, there exists some $r_3^{a_3} \in V(\Gamma(G))$ connected to exactly one of them. By $(*)$, exactly one of $P_{i(r_1)}^{\alpha(a_1,r_1)}$ and $P_{i(r_2)}^{\alpha(a_2,r_2)}$ is connected to $P_{i(r_3)}^{\alpha(a_3,r_3)}$, so these vertices of $\Sigma(G)$ cannot be equivalent: $\lambda(v_1) \neq \lambda(v_2)$.

Also, λ is surjective. For, if $w \in V(\Psi(G))$ has weight W, choose a prime power s^b such that $s^b \mid W$ but $s^{b+1} \nmid W$. Then there exists $P^j \in w$ such that $s^b \mid P^j$ but $s^{b+1} \nmid P^j$, so that $P^j = P_{i(s)}^{\alpha(b,s)}$ by definition. Hence, the equivalence class of s^b is mapped to w.

Finally, we verify that λ preserves weights. If $v \in V(\Delta(G))$ and $r^a \in v$ then, by the definition of $P_{i(r)}^{\alpha(a,r)}$, r^a divides the weight of $\lambda(v)$. Conversely, let s^b be a prime power divisor of the weight W of $\lambda(v)$ such that

$s^{b+1} \nmid W$. Then, as in the preceding paragraph, the equivalence class of s^b is mapped to $\lambda(v)$. Since λ is injective, $s^b \in v$ and hence s^b divides the weight of v. Consequently, λ is a weight-preserving isomorphism. ∎

After $\Delta(G)$ is constructed, we compute the standard name of G and the characteristic of G by following algorithmically the steps of the proof of Theorem 1.1, as described in Section 4. The quantities $|V(\Delta(G))|$, $L(G)$, $L_2(G)$, $L_3(G)$, and the 2- and 3-parts of the weights in $\Delta(G)$ can be computed in polynomial time. In particular, $|V(\Delta(G))|$ and $L_2(G)$ determine which of the Cases I–III the group G belongs to. Going through the argument in Case I, it is easy to see that the computation which determines the isomorphism type of G using these quantities can be performed in polynomial time. The only non-trivial step is to determine whether a weight w is divisible by a ppd$(p; k)$-prime, for a given prime p and integer $k > 6$. (Such steps are used in Propositions 4.2, 4.5, and 4.7.) This can be done, for example, by computing $r := \prod_{1 \le j \le k-1}(p^j - 1)$ and the greatest common divisor s of w and $p^k - 1$. The weight w is divisible by a ppd$(p; k)$-prime if and only if s does not divide r. The computations with the weights indicated in Cases II and III can be also done in polynomial time. This completes the proof of Theorem 1.2.

We conclude this section with a remark concerning the groups listed in Theorem 1.1. These groups are not quite characterized in terms of the graph $\Delta(G)$. It is, however, worth noting that the groups can be distinguished in polynomial time, using a little more data. We briefly indicate this in our five cases. Recall that an element g is said to have ppd$^{\#}(p; n)$-*order*, $n \ge 2$, if $|g|$ is divisible by a prime that divides $p^n - 1$ but not $p^i - 1$ for $1 \le i < n$ (cf. Section 3); such a prime exists unless either $p = 2$, $n = 6$ or p is a Mersenne prime and $n = 2$, in which cases we define ppd$^{\#}(p; n)$-order to mean that $|g|$ is divisible by 9 or 4, respectively; if $n = 1$ we define ppd$^{\#}(p; n)$-order to mean that $|g|$ is divisible by some factor of $p - 1$ greater than 2 (so the only pairs p, n we are excluding are $2, 1$ and $3, 1$).

(i) If $q = 3$ then the groups can be distinguished in polynomial time using Theorem 5.3. For larger values of q, see [AB], where elements of ppd$^{\#}(p, em)$- or ppd$^{\#}(p, 2em)$-order are used to distinguish these groups by a Monte Carlo algorithm.

(ii) The probability that an element g satisfies $g^{q+1} = 1 \ne g^2$ is at least $1/16$ in PSp$(4, q)$ but at most $1/q$ in PSL$(2, q^2)$. Hence these groups can be distinguished for all large enough q.

(iii) In P$\Omega^+(8, q)$ one of our chosen elements will (probably) have ppd$^{\#}(p, 4e) \cdot$ ppd$^{\#}(p, 2e) \cdot$ ppd$^{\#}(p, e)$-order, which occurs in neither PSp$(6, q)$ nor $\Omega(7, q)$ provided that $q > 3$.

(iv) The probability that an element g satisfies $g^{(q^2+1)/(2,q-1)} = 1 \neq g$ is at least $1/256$ in $\mathrm{PSp}(8,q)$ or $\Omega(9,q)$ but at most $1/q^4$ in $\mathrm{P}\Omega^-(8,q)$. Hence the first two groups can be distinguished from the third one for all large enough q.

(v) Use brute force.

5.4. *Is There a Practical Algorithm*?

Although the algorithm presented in Section 5.3 runs in polynomial time in the length of the input, it is totally impractical. There are three main sources of inefficiency: (I) the crude estimate in Theorem 5.5, which necessitates a large constant in the definition of the number N; (II) the appeal to Theorem 5.3; and (III) the order oracle assumed in the theorem. In this section, we indicate a more practical version of the algorithm, at least in the case when it is known that the input group is a classical simple group.

(*I*,*II*): *Decreasing N and avoiding Theorem* 5.3. For classical groups, we define $N = \lceil 144n^{3/2} \log n \rceil$ in place of the much larger bound used in Section 5.3. Also, the function $f(G)$ in Theorem 5.3 has more reasonable values for classical groups, so running the constructive recognition algorithm for $q < 1 + 5Nn$ requires $O(\mu n^c)$ time, with a constant c around 10 and "practical" constants hidden in the big-O notation. However, this is still not good enough for implementation, so we indicate a heuristic argument on *how to avoid Theorem* 5.3 *entirely* for classical groups. While Theorem 5.5 contains impractical bounds on q and on probability, undoubtedly much better bounds can be obtained, in which case the method described below will work efficiently for the exceptional groups as well.

As in Section 5.3, take N random elements of G, and collect their orders in a list L. We compute the prime numbers $p_1, \ldots, p_l$ less than $1 + 5Nn$ in polynomial time, and write each order $|g| \in L$ in the form $|g| = c_g \prod_{i=1}^{l} p_i^{\beta_i}$, with c_g relatively prime to $p_1, \ldots, p_l$. After that, we write the numbers c_g in the form $\prod_{i=1}^{m} P_i^{\alpha_i}$ with pairwise relatively prime P_i, as in the original algorithm. We compute at most $l + 1$ versions of the graph $\Delta(G)$: one using the element orders in L as in the original algorithm, and also for each p_j with $1 \leq j \leq l$ which divides some element order in L, using the numbers $c_g \prod_{i \neq j} p_i^{\beta_i}$ instead of the numbers $|g|$, for $|g| \in L$.

We claim that with probability at least $1 - 2/n$, one of the graphs we have computed is really $\Delta(G)$. The argument in the preceding section yields that, with probability at least $1 - 1/n$, the list L contains element orders divisible by $\mathrm{lcm}(r^a, s^b)$ for all pairs of prime powers necessary for the definition of $\Delta(G)$. If the (unknown) $q = p^e$ such that G is defined

over GF(q) satisfies $q > 1 + 5Nn$, then we have seen that, with probability at least $1 - 1/n$, p does not divide any of the element orders in L, so the construction of $\Delta(G)$ using the original element orders in L is correct. If $q \leq 1 + 5Nn$ then $p = p_j$ for some j with $1 \leq j \leq l$, and the construction using the numbers $c_g \prod_{i \neq j} p_i^{\beta_i}$ obtains the desired graph $\Delta(G)$.

For example, if $G \cong \mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5)$ then the element orders are 2, 3, and 5. This corresponds to a graph with three isolated vertices, with weights, 2, 3, 5, which, by Subcase 2 in Section 4.3, is not $\Delta(H)$ for any simple group H. Deleting the powers of 2 from the element orders, we obtain $\Delta(\mathrm{PSL}(2, 4))$ while deleting the powers of 5, we get $\Delta(\mathrm{PSL}(2, 5))$. Deleting the powers of 3 does not give $\Delta(H)$ for any simple group H, by Subcase 1 in Section 4.3.

However, we do not know in general how to prove that among the at most $l + 1$ graphs we constructed, none is isomorphic to $\Delta(H)$ for some simple group H not isomorphic to G. We formulate this question precisely. For any group G, we define the prime power graph $\Gamma^*(G)$ of G in the following way. The vertices of $\Gamma^*(G)$ are the prime powers occurring as element orders in G. Vertices r^a, s^b are connected if some $g \in G$ has order $\mathrm{lcm}(r^a, s^b)$. For a prime r occurring as a vertex in $\Gamma^*(G)$, we denote by $\Gamma^*(G)_r$ the graph obtained by deleting all powers of r from the vertex set of $\Gamma^*(G)$. After that, we define the weighted graphs $\Delta^*(G)$ and $\Delta^*(G)_r$ as the quotient graphs of $\Gamma^*(G)$ and $\Gamma^*(G)_r$, respectively, by using the equivalence classes of vertices with the same neighbors. In particular, if G is of Lie type of characteristic p then $\Gamma^*(G)_p = \Gamma(G)$ and $\Delta^*(G)_p = \Delta(G)$ as defined originally.

Conjecture 5.8. Let G, H be simple groups of Lie type, and let r be the characteristic of H. Then $\Delta^*(G) \ncong \Delta(H)$, and if $\Delta^*(G)_r \cong \Delta(H)$ then either $G \cong H$ or the pair $\{G, H\}$ is listed in Theorem 1.1.

(*III*): *Orders of elements*. Next we address the practicality of the assumption that we can compute element orders in G. In practice, black-box groups occur as permutation groups and matrix groups. Finding the characteristic is a problem only in the case of matrix groups. If $G \leq \mathrm{GL}(d, p^e)$ then there is a practical algorithm by Celler and Leedham-Green [CLG3] to compute element orders. This algorithm does not run in polynomial time if the order of the input element g is divisible by some large prime divisor of $p^i - 1$ for some i. However, if the characteristic of G is different from p, then by the results of Landazuri and Seitz [LS] and Feit and Tits [FT], the primes dividing $|G|$ are bounded from above by a polynomial function of the dimension d, so the algorithm in [CLG3] runs in polynomial time.

Therefore, we can run our algorithm for the construction of $\Delta(G)$; if we encounter an element such that we cannot compute its order then we

know that the characteristic of G is p. If the characteristic is known then the isomorphism type of G can be determined by a polynomial time Monte Carlo algorithm, without computing element orders, by computing a small fraction of the information used for the construction of $\Delta(G)$ [BKPS]. Once G is known, of course $\Delta(G)$ can be constructed.

ACKNOWLEDGMENT

We are indebted to N. Spaltenstein for the PSL$(2, q)$ case of Theorem 1.2, and for suggesting ideas for a different approach to the general case of that theorem.

REFERENCES

[Asch1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[Asch2] M. Aschbacher, Chevalley groups of type G_2 as the group of a trilinear form, *J. Algebra* **109** (1987), 193–259.

[AB] C. Altseimer and A. V. Borovik, Probabilistic recognition of orthogonal and symplectic groups, pp. 1–20 in [KS3].

[Ba] L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, *in* "Proc. ACM Symp. on Theory of Computing, 1991," pp. 164–174.

[BB] L. Babai and R. Beals, A polynomial-time theory of black-box groups I, *in* "Groups St. Andrews 1997 in Bath, vol. I," London Math. Soc. Lect. Note Series 260, pp. 30–64, Cambridge Univ. Press, Cambridge, UK, 1999.

[BGKLP] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks, and P. P. Pálfy, Short presentations for finite groups, *J. Algebra* **194** (1997), 79–112.

[BKPS] L. Babai, W. M. Kantor, P. P. Pálfy, and Á. Seress, Black-box recognition of finite simple groups of Lie type by statistics of element orders, in preparation.

[BDS] E. Bach, J. Driscoll, J. O. Shallit, Product refinement, *J. Algorithms* **15** (1993), 199–222.

[BLNPS] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress, A mélange of black-box algorithms for recognising finite symmetric and alternating groups I, submitted for publication.

[Bra] S. Bratus, "Recognition of Finite Black-Box Groups," Ph.D. thesis, Northeastern University (1999).

[BP] S. Bratus and I. Pak, Fast constructive recognition of a black-box group isomorphic to S_n or A_n using Goldbach's Conjecture, *J. Symbolic Comput.* **29** (2000), 33–57.

[Bro] P. A. Brooksbank, A constructive recognition algorithm for the matrix group $O(d, q)$, pp. 79–93 in [KS3].

[Bro2] P. A. Brooksbank, "Constructive Recognition of the Finite Simple Classical Groups," Ph.D. thesis, Univ. Oregon, 2001.

[BK] P. A. Brooksbank and W. M. Kantor, On constructive recognition of a black-box PSL(d, q), pp. 95–111 in [KS3].

[Car1] R. W. Carter, "Simple Groups of Lie Type," Wiley, London/New York/Sydney/Toronto, 1972.

[Car2] R. W. Carter, Centralizers of semisimple elements in the finite classical groups, *Proc. London Math. Soc.* **42** (1981), 1–41.

[Ce] F. Celler, "Matrixgruppenalgorithmen in GAP," Ph.D. thesis, RWTH Aachen, 1997.

[CLG1] F. Celler and C. R. Leedham-Green, A non-constructive recognition algorithm for the special linear and other classical groups, pp. 61–67 in [FK].

[CLG2] F. Celler and C. R. Leedham-Green, A constructive recognition algorithm for the special linear group, *in* "The Atlas of Finite Simple Groups: Ten Years On," London Math. Soc. Lect. Note Series 249, pp. 11–26, Cambridge Univ. Press, Cambridge, UK, 1998.

[CLG3] F. Celler and C. R. Leedham-Green, Calculating the order of an invertible matrix, pp. 55–60 in [FK].

[CLMNO] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien, Generating random elements of a finite group, *Comm. Algebra* **23** (1995), 4931–4948.

[CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, "Atlas of Finite Groups," Clarendon, Oxford, 1985.

[CFL] G. Cooperman, L. Finkelstein, and S. Linton, Recognizing $GL_n(2)$ in non-standard representation, pp. 85–100 in [FK].

[De] D. I. Deriziotis, The centralizers of semisimple elements of the Chevalley groups E_7 and E_8, *Tokyo J. Math.* **6** (1983), 191–216.

[DF] D. I. Deriziotis and A. P. Fakiolas, The maximal tori of the finite Chevalley groups of type E_6, E_7 and E_8, *Comm. Algebra* **19** (1991), 889–903.

[DM] D. I. Deriziotis and G. O. Michler, Character table and blocks of finite simple triality groups ${}^3D_4(q)$. *Trans. Amer. Math. Soc.* **303** (1987), 39–70.

[DLi] D. I. Deriziotis and M. W. Liebeck, Centralizers of semisimple elements in finite twisted groups of Lie type, *J. London Math. Soc.* **31** (1985), 48–54.

[FT] W. Feit and J. Tits, Projective representations of minimum degree of group extensions, *Canad. J. Math.* **30** (1978), 1092–1102.

[FK] L. Finkelstein and W. M. Kantor (Eds.), "Groups and Computation II," DIMACS Series in Discrete Math. and Theoretical Computer Science, Vol. 28, Am. Math. Soc., Providence, 1997.

[GL] R. M. Guralnick and F. Lübeck, On p-singular elements in Chevalley groups in characteristic p, pp. 169–182 in [KS3].

[HLOR1] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees, Testing matrix groups for primitivity, *J. Algebra* **184** (1996), 795–817.

[HLOR2] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees, Computing matrix group decompositions with respect to a normal subgroup, *J. Algebra* **184** (1996), 818–838.

[HR] D. F. Holt and S. Rees, Testing modules for irreducibility, *J. Austral. Math. Soc. Ser. A* **57** (1994), 1–16.

[HS] A. Hulpke and Á. Seress, Short presentations for three-dimensional unitary groups, *J. Algebra*, to appear.

[IY] N. Iiyori and H. Yamaki, Prime graph components of the simple groups of Lie type over the field of even characteristic, *J. Algebra* **155** (1993), 335–343.

[KM] W. M. Kantor and K. Magaard, Black-box exceptional groups of Lie type, in preparation.

[KS1] W. M. Kantor and Á. Seress, Black box classical groups, *Mem. Amer. Math. Soc.* **149** (2001), 708.

[KS2] W. M. Kantor and Á. Seress, Permutation group algorithms via black box recognition algorithms, *in* "Groups St. Andrews 1997 in Bath, vol. II," London

Math. Soc. Lect. Note Series 261, pp. 436–446, Cambridge Univ. Press, Cambridge, UK, 1999.

[KS3] W. M. Kantor and Á. Seress (Eds.), "Groups and Computation III," The Ohio State University Math. Research Inst. Publ., Vol. 8, de Gruyter, Berlin/New York, 2001.

[Kn] D. E. Knuth, "The Art of Computer Programming (Vol. 2): Seminumerical Algorithms," 2nd ed., Addison–Wesley, Reading, MA, 1981.

[Ko] A. S. Kondratev, On prime graph components of finite simple groups, *Mat. Sb.* **180** (1989), 787–797, 864. [In Russian.]

[LS] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.

[La] R. Lawther, The action of $F_4(q)$ on cosets of $B_3(q)$, *J. Algebra* **212** (1999), 79–118.

[LGO] C. R. Leedham-Green and E. A. O'Brien, Recognising tensor products of matrix groups, *Internat. J. Algebra Comput.*, to appear.

[Lü] F. Lübeck, Finding p'-elements in finite groups of Lie type, pp. 249–255 in [KS3].

[Lu] M. S. Lucida, The diameter of the prime graph of a finite group, *J. Group Theory* **2** (1999), 157–172.

[NP] P. M. Neumann and C. E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc.* (*3*) **65** (1992), 555–603.

[NiP1] A. C. Niemeyer and C. E. Praeger, Implementing a recognition algorithm for classical groups, pp. 273–296 in [FK].

[NiP2] A. C. Niemeyer and C. E. Praeger, A recognition algorithm for classical groups over finite fields, *Proc. London Math. Soc.* (*3*) **77** (1998), 117–169.

[Shi1] K. Shinoda, The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic 2, *J. Fac. Sci. Univ. Tokyo* **21** (1974), 133–159.

[Shi2] K. Shinoda, The conjugacy classes of the finite Ree groups of type F_4, *J. Fac. Sci. Univ. Tokyo* **22** (1975), 1–15.

[Sho] T. Shoji, The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic $p \neq 2$, *J. Fac. Sci. Univ. Tokyo* **21** (1974), 1–17.

[Suz] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* **75** (1962), 105–145.

[Wa] H. N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.

[Wi] J. S. Williams, Prime graph components of finite groups, *J. Algebra* **69** (1981), 487–513.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.